

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Shankar Sahai et al.

Serial No.: 09/614,867

Group Art Unit: 2154

Filed: July 12, 2000

Examiner: Chad Zhong

For: METHOD AND COMPUTER PROGRAM
FOR WEBSITE USER REDIRECTION

Atty. Doc. No.: 630-015

Honorable Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313

APPEAL BRIEF

S I R:

In support of the Notice of Appeal filed November 1, 2004 (attached as APPENDIX II. S.), the Assignee of the entire right, title, and interest of the subject application (the "Appellant") respectfully submits this Appeal Brief.

06/06/2005 JBALINAN 00000128 09614867

01 FC:2401

250.00 0P

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
TABLE OF AUTHORITIES.....	iv
I. Real Party in Interest.....	1
II. Related Appeals and Interferences.....	2
III. Status of Claims.....	3
IV. Status of Amendments.....	4
V. Summary of Claimed Subject Matter.....	6
A. Independent Claim 1.....	8
B. Independent Claim 9.....	11
C. Independent Claim 17.....	13
VI. Grounds of Rejection to be Reviewed on Appeal.....	14
A. 35 U.S.C. § 112 ¶ 1 (Claims 1-18).....	14
B. 35 U.S.C. § 112 ¶ 2 (Claims 1, 9, and 17).....	15
VII. Argument.....	16
A. Overview.....	16
B. The Examiner Has Not Met His Burden to Establish a Reasonable Basis to Question the Enabling Disclosure Provided for the Claimed Invention.....	18
C. The Examiner's Rejections Should Be Withdrawn Because the Examiner's Understanding of the Appellant's Invention is in Error.....	23
1. The Examiner Misunderstands the Novelty of the Present Invention.....	23

2.	The Examiner Misunderstands Client and Server-Side Programs as They Relate to the Present Invention.....	24
3.	Cookie Access and Functionality Are Implementation Issues.....	27
D.	The Examiner's 35 U.S.C. § 112 ¶ 1 Rejections Should Be Withdrawn Because the Specification Enables One Skilled in the Art to Make and Use the Present Invention Without Undue Experimentation.....	31
1.	The Appellant's Disclosure Enables All Pending Claims To One Reasonably Skilled in the Art.....	31
2.	The Previous Assignee Was in Possession of a Working Product Embodying the Claimed Invention.....	35
E.	The Examiner's 35 U.S.C. § 112 ¶ 2 Rejections Should Be Withdrawn Because the Claim Language Distinctly Claims the Present Invention.....	36
F.	The Amendment Dated October 29, 2004 Should Be Entered and the Application Should Be Allowed.....	38
1.	The Examiner's Own Statements Prove Novelty.....	38
2.	The Application is Ready for Allowance.....	39
APPENDIX I: CLAIMS LISTING.....		41
APPENDIX II: EVIDENCE.....		49
A.	Copy of the Assignment document and proof of Recordation	
B.	Amendment and Response, dated April 5, 2004	

- C. Final Action, mailed April 29, 2004
- D. Response to Office Action, dated October 29, 2004
- E. Advisory Action, mailed February 14, 2005
- F. Microsoft (MSDN) Article "Designing Secure ActiveX Controls"
- G. Sun Microsystems Article "Signed Applets, Browsers, and File Access," dated April 1998
- H. Windows IT Pro Article "IE Unauthorized Cookie Access"
- I. Microsoft Support Article ID: 258430 "Web Site May Retrieve Cookies from Your Computer," dated November 26, 2003
- J. Netscape Persistent Client State HTTP Cookies Preliminary Specification
- K. AT&T Bell Laboratories "Proposed HTTP State-Info Mechanism," dated August 25, 1995
- L. RFC 2109 - "HTTP State Management Mechanism," Standards Track, dated February 1997
- M. RFC 2965 - "HTTP State Management Mechanism," Standards Track, dated October 2000
- N. *United States v. Telectronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988)
- O. *In re Marzocchi*, 439 F.2d 220, 224, 169 USPQ 367, 370 (CCPA 1971)
- P. *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988)
- Q. *In re Paulsen*, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994)
- R. *Multiform Desiccants Inc. v. Medzam Ltd.*, 133 F.3d 1473, 1477, 45 USPQ2d 1429, 1432 (Fed. Cir. 1998)
- S. Notice of Appeal, dated October 29, 2004

APPENDIX III: RELATED PROCEEDINGS.....69

TABLE OF AUTHORITIES

CASES

1. *United States v. Telectronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988).
2. *In re Marzocchi*, 439 F.2d 220, 224, 169 USPQ 367, 370 (CCPA 1971).
3. *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988).
4. *In re Paulsen*, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994).
5. *Multiform Desiccants Inc. v. Medzam Ltd.*, 133 F.3d 1473, 1477, 45 USPQ2d 1429, 1432 (Fed. Cir. 1998).

STATUTES

1. United States Code, Title 35, §112.

SECONDARY SOURCES

1. Manual of Patent Examining Procedure, 8th Edition, §§ 2164-2165.
2. Manual of Patent Examining Procedure, 8th Edition, §§ 2106.01-2106.02.

I. REAL PARTY IN INTEREST

The real party in interest in the subject appeal is PalTalk Holdings, Inc., a privately-held company with a principal place of business at 213 West 35th St, 13th Floor, New York, NY 10001. PalTalk Holdings, Inc. is the Assignee of the entire, undivided interest of the subject application. The Assignment was made on December 19, 2001 from HearMe, Inc., the previous Assignee of the entire, undivided interest of the subject application, and was recorded on February 11, 2002 with the United States Patent and Trademark Office. A complete microfilm copy of the Assignment can be viewed at reel number 012602, frame number 0230. An accurate copy of the recorded Assignment is attached as APPENDIX II. A.

II. RELATED APPEALS AND INTERFERENCES

5 The Appellant is unaware of any prior or pending
appeal or any judicial or interference proceeding which may
directly affect, be related to, be directly affected by, or
have a bearing on the Board's decision in this proceeding.

10

III. STATUS OF CLAIMS

5 The subject application, as originally filed on July
12, 2000, contains Claims 1-18, with Claims 1, 9, and 17
being independent. All 18 claims stand finally rejected
under 35 U.S.C. § 112, first paragraph, for failing to
comply with the enablement requirement. In addition,
10 independent Claims 1, 9, and 17 stand finally rejected
under 35 U.S.C. § 112, second paragraph, as being
indefinite for failing to particularly point out and
distinctly claim the subject matter which the Appellant
regards as its invention. Appellant hereby appeals these
15 final rejections under 35 U.S.C. § 112 to the Board.

IV. STATUS OF AMENDMENTS

The Appellant received a first Office Action on the
5 merits dated October 6, 2003. The first Office Action on
the merits rejected all pending Claims 1-18 under 35 U.S.C.
§ 112, first paragraph, for failing to comply with the
enablement requirement. In addition, the first Office
Action on the merits separately rejected independent Claims
10 1, 9, and 17 under 35 U.S.C. § 112, second paragraph, as
being indefinite. The Appellant timely responded to the
October 6, 2003 Office Action with an Amendment and
Response dated April 5, 2004. In this Amendment and
Response, Appellant amended independent Claims 1, 9, and 17
15 to more clearly claim the present invention. The Appellant
also traversed the Examiner's enablement rejection and
argued that the Examiner's understanding of the present
invention was in error.

Appellant then received a Final Action dated April 29,
20 2004 finally rejecting all pending Claims 1-18 under 35
U.S.C. § 112, first paragraph, for failing to comply with
the enablement requirement. The Final Action again
separately rejected independent claims 1, 9, and 17 under
35 U.S.C. § 112, second paragraph, for failing to

particularly point out and distinctly claim the subject matter which the Appellant regarded as its invention.

Appellant timely filed a Response to the Final Action and a Notice of Appeal, both dated October 29, 2004.

5 Appellant's Response again clarified the claim language of independent Claims 1, 9, and 17 and again traversed the Examiner's enablement rejection. An Advisory Action was mailed on February 14, 2005 which refused entry of the Response to the Final Action dated October 29, 2004 stating
10 that the Response "does not deem to place the application in better form for appeal by materially reducing or simplifying the issues for appeal."

The April 5, 2004 Amendment and Response, the April 29, 2004 Final Action, the October 29, 2004 Response to
15 Final Action (not entered), and the February 14, 2005 Advisory Action are attached as Appendices II. B., II. C., II. D., and II. E., respectively.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In many instances, visitors to an Internet website
5 receive offers and solicitations for some product or
service. These offers and solicitations come in many
forms, including pop-up advertisements, banner
advertisements, and various sign-up and subscription forms.
Visitors often become annoyed by these frequent offers and
10 solicitations, particularly when visitors receive duplicate
offers and solicitations for the same product or service.
In addition, these offers and solicitations may not be
relevant in many instances. For example, it is
particularly vexing to a visitor of a website who has
15 already purchased a product or subscribed to a service to
nevertheless receive solicitations for that product or
service. Not only can these offers and solicitations waste
valuable network bandwidth, they cause the visitor to the
website to needlessly waste time and expend effort to
20 arrive at the appropriate website relating the product or
service.

The present invention makes use of "cookies" to
automatically redirect a visitor who has already purchased
a product or subscribed to a service to an appropriate

website. This redirection is useful to avoid duplicate offers and solicitations.

The present invention is also important for vendor control and management. The present invention makes use of
5 custom client or server-side programs to place these cookies on a user's machine after the user has purchased, installed, or subscribed to a particular product or service. Then, when the user subsequently activates a link to purchase another product or utilize the same service,
10 the client or server-side program of the present invention may search the user's machine for relevant cookies. The present invention then makes a determination (from data stored within any relevant cookies that were located) if the user already possesses the product or has subscribed to
15 the service identified by the link the user has just activated. If the present invention determines that the user already possesses the product or has subscribed to the service, the client or server-side program of the present invention may redirect the user to another website (perhaps
20 the website associated with the specific vendor, product, or service). This website may be determined from data stored within the cookie on the user's machine. If the present invention determines that the user does not possess the product or service, the user may be allowed to follow

the activated link and interact with the offer or solicitation.

The present application contains Claims 1-18, of which Claims 1, 9, and 17 are independent. Claims 1-18 are reproduced in their finally rejected form in APPENDIX I. The following briefly summarizes the claimed invention as set forth in each independent claim. The disclosed corresponding structure for any means-plus-function elements is also set forth below.

A. Independent Claim 1

Claim 1 is directed to a method for website redirection. The method entails five distinct steps. The first step recites "providing, by a second Web site, a URL offering a product or service, said URL specifying a program on the second Web site." (Claim 1). The Appellant discloses several ways to provide this "URL offering a product or service." *Id.* These mechanisms for providing this URL to a user include a traditional hyperlink found on a website, an email sent to a user, or a separate executable computer program. (Specification, "Web Product and Service Offerings," pp. 8-9, as well as Figure 2).

The "program on the second Web site" as recited in the first step of independent Claim 1 is disclosed by the

Appellant under the "Client Side and Server Side Programs" heading on page 12 of the Specification. The Appellant teaches a program residing either on the "client side or the server side" that "reads cookie 302 and determines whether user 102 possesses the product or service."

(Specification, p. 12, ll. 2-4). The Appellant even provides several advantageous and disadvantages to each implementation scheme (i.e., the use of server-side versus client-side programming). The Appellant further discloses several examples of server-side web programs, any of which could be used to read the cookie located on the user's computer, including "Common Gateway Interface (CGI) scripts, Java servlets, Hypertext Preprocessor (PHP) scripts, Perl scripts, and the like." (Specification, p.

12, ll. 8-10). The Appellant also discloses several examples of client-side web programs, which could alternatively be used to perform the cookie reading step of Claim 1, including "Java applets, Java scripts, Active X controls and the like." (Specification, p. 12, ll. 17-19).

The second step found in independent Claim 1 recites "reading, by said program, a cookie located in the user's computer in response to the user activating said URL." (Claim 1). The Specification teaches that the cookie, which is merely a text file on a client computer, is read

by a client-side or server-side program. As described above, numerous examples of these programs are given within the Specification. These web programs are capable of performing any task a person actually sitting at the user's computer can perform, including reading text files, or cookies. Support for this step is found within the Appellant's disclosure under the "Cookies" heading. (Specification, pp. 9-11, ll. 18-27).

The third and fifth steps recited in independent Claim 1 involve making a positive or negative determination as to whether the user already possesses a particular product or service. The Appellant discloses "several ways" to make this determination. (Specification, p. 10, l. 14). One way involves "searching the cookie for the name of the product or service." (Specification, p. 10, ll. 14-15). Another way to make this determination comprises "searching the cookie for a URL where the product or service can be acquired." (Specification, p. 10, ll. 15-16).

Step four entails "redirecting, by said program" the user to a first or second website depending on whether the determination was positive or negative. (Claim 1). Website redirection by a client-side or server-side program is described in detail under the "Redirecting" heading within the Appellant's disclosure. "Standard HTTP redirect

protocol" is one example of redirection taught in the specification. (Specification, p. 11, ll. 14-27). An example is also given within the specification to elucidate the website redirection step.

5

B. Independent Claim 9

Independent Claim 9 is directed to a system for website redirection. As in independent Claim 1, independent Claim 9 contains five distinct limitations. In fact, the five system limitations recited in independent Claim 9 track the method limitations of independent method Claim 1. For example, the first limitation of independent Claim 9 requires "means for providing...a URL offering a product or service to the user." As described above for independent Claim 1, the Appellant's disclosure recites several mechanisms for providing and presenting a URL to a user of the system. These mechanisms may include providing the URL through a traditional hyperlink found on a website, an email sent to a user, or providing the URL in a separate executable computer program. (Specification, "Web Product and Service Offerings," pp. 8-9, as well as Figure 2).

The second limitation of independent Claim 9 recites "means for reading...a cookie located on the user's computer." As described above for independent Claim 1,

this is described in greater detail within the Specification under the "Cookies" heading. (Specification, pp. 9-11). The Appellant discloses various functions that may be used by the server-side or client-side program to
5 read a cookie, including standard text input and scanning (as supported by all computer systems) and searching for various strings, including the name of a product or service or a specific URL contained within the cookie. (Specification, p. 10, ll. 14-16).

10 The third limitation of independent Claim 9 requires "means for providing a positive determination...as to whether the user already possesses said product or service is true." As described above for independent Claim 1, the Appellant discloses several ways to make this
15 determination. (See Specification, p. 10, ll. 14-16).

The fourth limitation of independent Claim 9 recites "a means for redirecting...the user" to a particular website upon a positive determination in the previous limitation. As described above for independent Claim 1,
20 the Appellant discloses the use of "Standard HTTP redirect protocol" as one method of website redirection. An example is also given within the Specification to elucidate the website redirection functionality. (Specification, p. 11, ll. 14-27).

Finally, the fifth limitation of independent Claim 9 requires a "means for offering...to supply said product or service to the user" upon a negative determination in the third limitation. The Appellant discloses several

5 mechanisms "to supply user 102 with the product or service. This can be accomplished by providing a Web page or other type of media via Web site 104 that offers the product or service to user 102." (Specification, p. 13, ll. 6-9). The Appellant further discloses that the product or service may
10 be "downloaded via Web site 104 or acquired via some other manner such as receiving it via e-mail or by postal mail. (Specification, p. 13, ll. 12-13).

C. Independent Claim 17

15 The final independent claims, Claim 17, is directed to "a computer program product" for website redirection. As in Claims 1 and 9, independent Claim 17 contains five limitations. In fact, these five limitations, which are the same as the five limitations found in independent Claim
20 9 except that each limitation in Claim 17 is implemented within a "computer readable program code." Support for these five limitations is similarly found within the Appellant's disclosure. In particular, the Appellant provide an overview of the "computer readable program code"

as server-side or client-side programs under the heading
"Client Side and Server Side Programs" on page 12 of the
Specification. Each individual claim limitation can be
found in the corresponding location as discussed above for
5 independent Claim 9.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Appellant hereby appeals to the Board the
10 Examiner's final rejections as set forth in the Final
Action dated April 29, 2004 and in the Advisory Action
dated February 14, 2004 (attached as Appendices II. C. and
II. E., respectively). The grounds of rejection to be
reviewed on appeal are as follows:

15

A. 35 U.S.C. § 112, ¶ 1 (Claims 1-18)

The Examiner finally rejected Claims 1-18 under 35
U.S.C. § 112, first paragraph, for failing to comply with
20 the enablement requirement. In the opinion of the
Examiner, "the claims contain subject matter, which was not
described in the specification in such a way as to enable
one skilled in the art to which it pertains, or which it is
most nearly connected, to make and/or use the invention."
25 (April 29, 2004 Final Action, p. 2). The Examiner further
opined that "applicants fail to teach the specific methods

which allow the program in the second website to read the first website's cookie stored in the user's computer."

(April 29, 2004 Final Action, p. 3).

5 **B. 35 U.S.C. § 112, ¶ 2 (Claims 1, 9, and 17)**

The Examiner separately finally rejected Claims 1, 9, and 17 under 35 U.S.C. § 112, second paragraph, for "failing to particularly point out and distinctly claim the subject matter which the applicant regards as the

10 invention." (April 29, 2004 Final Action, p. 4). According to the Examiner, the words "positive" and "negative" are "murky or not clearly understood." (April 29, 2004 Final Action, pp. 4-5)

VII. ARGUMENT

A. Overview

5 The Appellant respectfully submits that the Examiner
has misunderstood and failed to appreciate the novelty of
the Appellant's invention. The Appellant believes that the
Examiner's confusion may be attributed to the innovative
10 and original manner in which the Appellant's invention
utilizes Internet "cookies." Conventional Internet
applications, such as web browsers including Microsoft's
Internet Explorer and Netscape's Communicator browser, do
not inherently support the novel cookie functionality of
15 the Appellant's invention. The Appellant's invention (as
the Examiner has made clear in his rejections) is quite
unlike traditional Internet applications because the
Appellant's invention may allow for inter-domain cookie
access and sharing of cookies between websites. The
20 Appellant's invention enables this unique cookie
functionality through the use of server-side and client-
side programs (such as ActiveX controls, Java applets, CGI
scripts, and the like), which are fully disclosed and
enabled in the Appellant's Specification. As discussed
25 *infra*, these server-side and client-side programs are

capable of performing all the enhanced cookie functionality required by the Appellant's claimed invention.

The Appellant will show that: 1) the Examiner has failed to meet his burden to show that applicant's disclosure is non-enabling; 2) the Examiner inappropriately limited the Appellant's invention to traditional Internet "cookies" and their corresponding customary functionality; 3) the Examiner failed to consider the Appellant's use of custom server-side and client-side programs; 4) the Examiner's arguments are biased in favor of popular, traditional Internet cookie applications; and 5) cookie access, management, and functionality are an application implementation issue. Appellant will also show that the subject application fully enables one skilled in the art to make and use the Appellant's invention without undue experimentation and that the claim language is definite, clear, and readily understood.

In addition, the Appellant will disclose a web-based software product that was fully-functioning before the filing of the subject application. This software product embodied Claims 1-18 of the present invention and was marketed and sold by HearMe, Inc., the subject application's previous Assignee. The Appellant's arguments will conclude with a summation detailing why the Examiner's

rejections should be withdrawn and why the application is ready to issue.

5 **B. The Examiner Has Not Met His Burden
 to Establish a Reasonable Basis to
 Question the Enabling Disclosure Provided
 for the Claimed Invention**

10 The Examiner, before making an enablement rejection
under 35 U.S.C. § 112, has the initial burden to establish
a reasonable basis to question whether the applicant's
disclosure for the claimed invention is enabling or not.
(see MPEP § 2164.04). The Examiner must consider the
15 evidence *as a whole*, including such factors as: (a) the
breadth of the invention(s); (b) the nature of the
invention(s); (c) the state of the prior art; (d) the level
of one of ordinary skill; (e) the level of predictability
in the art; (f) the amount of direction provided by the
20 inventor(s); (g) the existence of working examples; and (h)
the quantity of experimentation needed to make or use the
invention based on the content of the disclosure.

As stated by the CAFC, "it is incumbent upon the
Patent Office, whenever a rejection on this basis is made,
25 to explain why it doubts the truth or accuracy of any
statement in a supporting disclosure and to back up
assertions of its own with acceptable evidence." See *In re*

Marzocchi, 439 F.2d 220, 224, 169 USPQ 367, 370 (CCPA 1971), attached as APPENDIX II. O.

In the Examiner's April 29, 2004 Final Action, the Examiner cites a host of Internet articles and
5 publications, including the "Netscape Persistent Client State HTTP Cookies Preliminary Specification." APPENDIX II. J. Citing the Netscape Preliminary Specification, the Examiner argued that, "a cookie can only be read and modified by an object in the valid domain and path defined
10 in the cookie when it was created." (April 29, 2004 Final Action, p. 3). The Examiner further opined, "in order to implement the claimed invention, it requires the program from the second domain [second website] to read the cookie from the first domain [first website]. As such, it is not
15 clear how the claimed invention can be implemented while still following the specification of the HTTP Cookies." (April 29, 2004 Final Action, p. 3).

The Appellant agrees with the Examiner that traditional web browsers may have no built-in support for
20 sharing cookies between domains. The Appellant respectfully contends, however, that the present invention uses client-side or server-side programs to access, read, write, and otherwise manipulate its cookies. Nothing in the claims or disclosure limits the Appellant's invention

to traditional web browser functionality. In fact, the subject application discloses the novel use of "a client side program or a server side program" to create, read, and place cookies on a user's computer. (Specification, p. 9, 11. 14-15). These programs work in conjunction with traditional web browser applications, as traditional browsers typically do not include these programs. Thus, the Appellant's invention may supplement and expand upon traditional web browser functionality.

Further, nothing in the Appellant's disclosure suggests that the Appellant's invention is limited to cookies as defined by Netscape's Persistent Client State HTTP Cookies Preliminary Specification. In fact, the Appellant's specification provides a "Terminology" heading that explicitly defines the term "cookie" as "information that is located on a user's computer for later use by a Web site." (Specification, p. 5, 11. 24-26). Appellant also gives an example of a "cookie" in the specification as "a text file." (Specification, p. 5, 11. 26-27). The Netscape HTTP Cookies Preliminary Specification is just one of many HTTP cookie specifications. In fact, the Netscape Preliminary Specification cited and quoted by the Examiner is now rendered obsolete by several subsequent cookie specifications, including RFC 2109 and RFC 2965, published

February 1997 and October 2000, respectfully (attached as APPENDIX II. L. and APPENDIX II. M.).

Since the Appellant defines a "cookie" broadly enough to cover any "information that is located on a user's

5 computer for later use by a Web site," the Appellant is not limited to the Netscape cookie specification or any other publicly available cookie specification. (Specification, p.

5, ll. 24-26). Although the Appellant's invention is compatible with such traditional cookies and works with

10 such traditional cookies, the Appellant provides a full and complete disclosure to support the Appellant's own cookie specification. The Appellant provides a section labeled

"Cookies" on pages 9-11 of the Specification detailing the precise cookie operations in accordance with the present

15 invention. Namely, with regard to cookie creation and placement on a user's computer, the Specification reads:

"cookie 302 can be placed on the computer of user 102 by either a client side of server side program."

(Specification, p. 9, ll. 14-15, emphasis added). With

20 regard to cookie analysis and reading, the Specification

further states: "the cookie sought by the program is a cookie relating to the product or service being offered by Web site 106." (Specification, p. 13, ll. 28-30, emphasis

added). Under the "Environment" section starting on page

14 of the Specification, the Appellant emphatically states that "the functions performed by the computers of user 102, Web site 104, and Web site 106 are preferably implemented in software." (Specification, p. 14, ll. 29-30, emphasis added). Accordingly, the Appellant's cookie management functions are performed by custom server-side or client-side programs that expand upon traditional cookie management functionality.

A patentee is entitled to be his or her own lexicographer and may rebut the presumption that claim terms are to be given their ordinary and customary meaning. (See *In re Paulsen*, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994), attached as APPENDIX II. Q.). The Appellant submits that the definition of "cookie" disclosed in the present application is readily understood and "sufficiently clear in the specification that any departure from common usage would be so understood by a person of experience in the field of the invention." (See *Multiform Desiccants Inc. v. Medzam Ltd.*, 133 F.3d 1473, 1477, 45 USPQ2d 1429, 1432 (Fed. Cir. 1998), attached as APPENDIX II. R.).

Thus, the Appellant submits that the Examiner erroneously relied on traditional cookie functionality from traditional cookie specifications in making his enablement

rejection. Rather, the present invention utilizes client-side or server-side programs (such as Java applets, ActiveX controls, etc.) in conjunction with traditional web browser applications to support special cookie management

5 functionality. Therefore, the Appellant submits that the Examiner's rejections are misguided. The Examiner failed to meet his initial burden of establishing a reasonable basis for questioning the enablement of the claimed invention and failed to rely on all available

10 considerations as required by MPEP §§ 2164.01-2164.06. To the contrary, the Appellant further submits that Appellant's disclosure fully enables all pending Claims 1-18.

15

C. The Examiner's Rejections Should Be Withdrawn Because the Examiner's Understanding of the Appellant's Invention is in Error

20

1. The Examiner Misunderstands the Novelty of the Present Invention

The Appellant respectfully contends that the Examiner
25 has misunderstood the present invention and overlooked the present invention's novelty. The present invention utilizes cookies in new and unobvious ways. The Appellant realizes and fully understands that traditional web

browsers may not inherently support the cookie
functionality disclosed in the present application.

Accordingly, the Appellant has fully and adequately
disclosed custom server-side and client-side programs,

5 which may run on the client computer and/or on a server or
host, to perform the unique cookie management tasks that
traditional web browsers may be unable to perform. The
Examiner is undoubtedly aware that custom server-side and
client-side programs are not limited to cookie management

10 functionality as supported by traditional web browsers. In
fact, authorized or trusted server-side and client-side
programs may perform any task a user actually sitting at
the client or server workstation can perform. This
includes all the functionality required by the present

15 invention, including file access, directory and file
searching, and website redirection. As discussed *supra*,
the Examiner has misunderstood and improperly limited the
Appellant's invention to traditional cookies and
traditional cookie functionality in forming his enablement
20 rejections. This is simply not the purpose of the present
invention. In contrast to the Examiner's interpretation of
the present invention, the Appellant has invented a novel,
unobvious system and method for enhanced cookie support and

utilization, which is fully disclosed and enabled by the Appellant's specification.

5

2. The Examiner Misunderstands Client-Side and Server-Side Programs as They Relate to the Present Invention

10 The Appellant further submits that the Examiner misunderstands and incorrectly interprets the Appellant's disclosure as limited to traditional cookie functionality from traditional cookie applications (i.e., the cookie functionality present in most common web browser applications today). However, a careful review of the Appellant's disclosure reveals that the Appellant's invention is not limited to such traditional cookie functionality. In fact, one aspect of the novelty of the present invention is the custom, unique cookie management applications and programs, which are fully and adequately disclosed by the Appellant. Specifically, to create a cookie, the Appellant's disclosure states that "cookie 302 can be placed on the computer of user 102 by either a client-side or a server-side program." (Specification p. 9, 11. 14-15, emphasis added). To read and search for cookies, the Appellant's disclosure states that "a program

searches for a relevant cookie on the computer of user
102...the program then determines from the cookie whether
user 102 already possesses the product or service."

(Specification p. 7, ll. 22-25, emphasis added). Thus all
5 cookie creation and management functionality is handled by
these programs.

These client-side or server-side programs are fully
disclosed in detail beginning on page 12 under a separate
heading within the Appellant's specification entitled
10 "Client Side and Server Side Programs." Many examples of
these programs are also given in the specification,
including "Common Gateway Interface (CGI) Scripts, Java
servlets, Hypertext Preprocessor (PHP) scripts, Perl
Scripts...Java applets, Java scripts, ActiveX controls and
15 the like." (Specification, p. 12, ll. 9-19). These types
of server-side and client-side programs and their
functionality are common and well-known in the art.

Further evidence of the Appellant's intent not to
limit the present invention to traditional web browser
20 applications is found in the claims themselves. Each of
independent Claims 1 and 9 recite cookie management
functionality as being performed "by said program" residing
"on the second Web site." In independent Claim 17, the
cookie functionality is provided by "computer readable

program code means." Appellants submit that these are custom designed client-side or server-side programs. These custom programs may not be built-in to traditional web browsers (although the present invention contemplates that they may be packaged as such for sale). Similarly, the Appellant contends that the functionality of these custom programs is not inherent in traditional web browsers and these programs must be installed, configured, or otherwise utilized in accordance with the present invention to perform the cookie functionality described in the present invention.

3. Cookie Access and Functionality Are Implementation Issues

Even if the Examiner construed the present application as limited to traditional cookies, several different specifications exist for HTTP state management. Among these are Netscape's Preliminary Cookie Specification, Kristol's State-Info proposal (Appendix II. K.), RFC 2109 (Appendix II. L.), and RFC 2965 (Appendix II. M.). Even though most of these specifications teach that cookies should not be shared between different domains because of privacy and/or security concerns, these specifications do not preclude all access of another website's cookie

information. For example, RFC 2965 fully supports the access of cookies from and between two hosts (e.g., "host1.foo.com" and "host2.foo.com") even though the two hosts may comprise two completely separate websites as described in the present invention. (Appendix II. M., RFC 2965, § 7.1, p. 17). This cookie functionality would be completely supported by the traditional cookie specification and Internet standard. Under § 7.3 of RFC 2965, entitled "Unexpected Cookie Sharing," the specification reads:

A user agent SHOULD make every attempt to prevent the sharing of session information between hosts that are in different domains. Embedded or in-lined objects may cause particularly severe privacy problems if they can be used to share cookies between disparate hosts...User agent implementors are strongly encouraged to prevent this sort of exchange whenever possible." (Appendix II. M., p. 18, emphasis added).

Thus, it is clear from RFC 2965, which is regarded as the current *de facto* standard for HTTP state management, that cookie security and inter-domain access is an implementation issue. The user agent is responsible for handling all cookie management functions. For clarification, one web browser application provider (e.g., Microsoft's Internet Explorer) may choose to follow the privacy guidelines as outlined in RFC 2965, while another

web browser application provider may not. Just because sharing cookies across different domains is something discouraged due to privacy or security concerns, it is not "impossible."

5 Rather, the Appellant respectfully submits that there are many instances where even Microsoft's Internet Explorer browser allows inter-domain cookie access. For example, Microsoft Knowledge Base (KB) article reports that "when you use Internet Explorer to visit a Web site, the Web site
10 may be able to retrieve cookies that were not created by that Web site from your computer." (See Appendix II. I.) Although the Appellant realizes that this was unintended behavior, it nevertheless supports the Appellant's position that this functionality is possible. Another example of
15 Microsoft Internet Explorer's cookie sharing between different Web sites is documented in Appendix II. H. in an article entitled "IE Unauthorized Cookie Access." The article states:

20 By design, the IE security model restricts cookies so that they can be read only by sited within the originator's domain. However...it is possible for a malicious web site operator to gain access to another site's cookie and read, add or change them."
25 (Appendix II. H., emphasis added).

Again, although this may be unintended behavior (i.e., a "bug" in Internet Explorer), it is clear that different web

browsers may utilize different security models that may allow or prohibit inter-domain cookie access. Contrary to the Examiner's position, this functionality is possible and is merely a browser implementation issue.

5 Further, several HTTP state management specifications have little or no security provisions relating to inter-domain access. David M. Kristol's "Proposed HTTP State-Info Mechanism" (Appendix, II. K.), which is often referred to as the precursor to the common Internet cookie,
10 discloses a request/response header. This header is called State-Info and carries state information back and forth between servers and client computers. The specification states that information within headers is completely unprotected:

15 The information in the State-Info headers is unprotected. Two consequences are:
1. Any sensitive information that is conveyed in a Sate-Info header is exposed to intruders.
20 2. A malicious intermediary could alter the State-Info header as it travels in either direction, with unpredictable results. (Appendix II. K., p. 7).

25

Applicant further submits that, depending on which cookie implementation an application provider is utilizing, inter-domain access may be supported. Hence, the Examiner relied on the most prevalent cookie implementation as

installed on the majority of client computers utilizing the most popular Internet browsers in forming his enablement rejection. No consideration of the state of the art at the time of filing or the level of experimentation required by one skilled in the art was considered or analyzed by the Examiner.

10 **D. The Examiner's Rejections Should Be Withdrawn
Because the Specification Enables One Skilled in
the Art to Make and Use the Present Invention
Without Undue Experimentation**

15 **1. The Appellant's Disclosure Is Enabling To
One Reasonably Skilled in the Art**

The Appellant submits that the present invention as disclosed is fully enabling as required by the 35 U.S.C. § 112. The Examiner, in the April 29, 2004 Final Action, stated:

25 In order to implement the claimed invention, it requires the program from the second domain [second website] to read cookies from the first domain [first website]. However, according to the specification of HTTP Cookies as set forth hereinabove, no other website [the second website] can read the first website's cookie. As such, it is not clear how the claimed invention can be
30 implemented while still following the specification of the HTTP cookie." (April 29, 2004 Final Action, p. 3, emphasis added).

As pointed out in response to this Final Action (APPENDIX II. D.) as well as *supra* within section "**VII. Arguments,**" there is no need to follow "the specification of the HTTP cookie" as the Examiner contends. Rather, the Appellant
5 has created and disclosed a novel cookie specification in the present application utilizing custom designed server-side and client-side programs.

According to independent Claims 1, 9, and 17, the present invention comprises five basic steps or
10 limitations. The support for each of these steps or limitations is found in the Appellant's original disclosure, as outlined above in section "**V. Summary of Claimed Matter**" above, and summarized as follows:

1. The first step or limitation is to provide a URL
15 offering a product or service to the user. This step is regularly performed at e-commerce websites and via email everyday. A simple hyperlink within an email or a hyperlink presented on a website will satisfy this step.

20 (See Specification, "Web Product and Service Offerings" heading, pp. 8-9, as well as Figure 2).

2. The second step or limitation is for a program to read a cookie located on the user's computer in

response to the user activating the URL.

(Specification, p.11, ll. 14-27). While cookie access via traditional web browsers is limited to certain domain paths, Appellants novel server-side and client-side programs have no such limitation. Rather, server-side and client-side programs are capable of accessing any file on a user's or server's computer, including traditional cookies.¹ (See Specification, p. 12, "Client Side and Server Side Programs"). Server-side or client-side programs can access cookies from any website, regardless of which website

¹ For example, it is well-known in the art that Java's Security Manager allows signed and/or trusted Java applets and applications to access local file resources once downloaded. According to an article by Sun Microsystems, Inc., dated April 1998, "by default, applets have no access to system resources outside the directory from which they were launched, but a signed applet can access local system resources as allowed by the local system's security policy. End users...can define their local security policy by specifying in a policy file how much access to local system resources a signed applet or application can have." (See APPENDIX II. G., p. 1). Likewise, as another example, any Microsoft ActiveX control can perform any task that the user of a client system can perform. This includes reading and writing local files, including traditional cookies. According to an article by Microsoft Corporation, "an ActiveX control can be an extremely insecure way to provide a feature. Because it is a Component Object Model (COM) object, it can do anything the user can do from that computer. It can read from and write to the registry, and it has access to the local file system." (See APPENDIX II. F., p. 1).

created the cookie. ActiveX controls and Java applets used to access the file system were well-known to those reasonably skilled in the art at the time of the present invention. Numerous examples of such applets, applications, and programs were widely available on the Internet as of the filing of this application.

3. The third step or limitation entails determining from the cookie whether the user already possesses a product or service. Several ways of making this determination, including searching relevant cookies for product name, unique identifiers, and URLs, are taught in the subject application. (Specification, p.10, 11. 14-16).

4. The fourth step or limitation entails redirecting the user to a website depending upon the determination in step or limitation 3 above. The present application discloses the use of "standard HTTP redirect protocol" to accomplish this step or limitation. (Specification, p. 11, 11. 14-15). The Specification also teaches of a specific redirection scheme whereby a web site supplies a URL to be embedded within a cookie. According to the Appellant's disclosure, "in

response to the HTTP request, Web site 106
replies with a URL to Web site 104. User 102 is
then presented with Web site 104.”
(Specification, p. 11, ll. 17-20).

5 5. The fifth and final step or limitation is
directed at offering a product or service to the
user if the determination from step 3 is
negative. This is fully described in the
specification and is typically performed by
10 presenting the user with an e-commerce website,
where the user might subscribe or purchase a
product or service. (Specification, p. 8, “Web
Product and Service Offerings). A simple website
displaying a product or service with input fields
15 for user information is all that is required to
perform this step.

20 **2. The Previous Assignee Was in Possession
of a Working Product Embodying the
Claimed Invention**

Not only is the specification enabling, but the
previous assignee of the present application, HearMe, Inc.
25 (“HearMe”)—once a leader in voice-over-IP communications—
shipped a product embodying all the elements of Claims 1-18

of the subject application in July 2000. VoiceCONTACT 2.0 SDK was a web-based software platform that offered high-quality live voice technology for talking to any number of friends (i.e. clients) simultaneously over the Internet or a private network. Since HearMe sold its VoiceCONTACT product line to several vendors, HearMe developed the present invention to assist in vendor control. With the help of cookies or other tokens that uniquely identified the selling vendor, clients who downloaded the product from particular selling vendors were able to see vendor-specific websites when using the VoiceCONTACT product (e.g., when a user received an email with the "Talk to Sender" invite link). A client-side ActiveX control read the cookies on the user's computer and redirected the user to the appropriate vendor's VoiceCONTACT website. Several other advantageous uses of the present invention were also evident.

E. The Examiner's 35 U.S.C. § 112 ¶ 2 Rejections Should Be Withdrawn Because the Claim Language Distinctly Claims the Present Invention

In the Final Action mailed April 29, 2004, the Examiner rejected Claims 1, 9, and 17 as "indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention."

(April 29, 2004 Final Action, p. 4). Specifically, in the opinion of the Examiner, the terms "positive" and

5 "negative" are "murky or not clearly understood." *Id.* The Examiner asked, "does positive mean true when determination from cookie whether the user already possesses product or service?" *Id.* In response, Appellant traversed this

rejection arguing that the claim language is definite and
10 clearly understood. (Amendment and Response dated April 5, 2004, p. 7). In addition, element (3) of Claim 1, was amended to read, "providing a positive determination when an inquiry by said program, from said cookie, as to whether the user already possesses said product or service is

15 true." (Amendment and Response dated April 5, 2004, p. 2).

Put another way, if the determination is made that a user already possesses the product or service, this is a positive determination. Likewise, if the determination is made (from analyzing cookie data) that the user does not

20 possess the product or service, this determinations is negative. Remarks made by the Appellant in the Amendment and Response dated April 5, 2004 made this clear. Namely, the Appellant stated, "Applicants have amended Claims 1, 9, and 17 to more clearly recite that 'positive' means 'true'

and 'negative' means 'false.'" (Amendment and Response dated April 5, 2004, p. 7).

The Appellant similarly submits that independent Claims 9 and 17 are also definite and clear. These claims, as amended, are unambiguous and logical: namely, a positive determination means the user already possess the product or service and a negative determination means the user does not possess the product or service. Accordingly, the Appellant respectfully submits that no uncertainty is created by the use of the terms "positive" and "negative." The Appellant has distinctly claimed the present invention, and the Examiner's rejection should be withdrawn.

**F. The Amendment Dated October 29, 2004
Should Be Entered and the Application
Should Be Allowed**

**1. The Examiner's Own Statements
Prove Novelty**

The Examiner's own statements support the novelty of the present invention. In making his enablement rejections, the Examiner admitted that no system or method exists to perform the claimed invention. In fact, the Examiner labeled the present invention as "impossible." (See April 29, 2004 Final Action, p. 5). This suggests that even the Examiner views the present invention as truly

unique and innovative. Accordingly, the only references cited by the Examiner are references showing traditional cookie access and functionality from conventional web applications. These references are all quite different
5 from the present invention, which utilizes server-side or client-side programs to read cookies created from other websites to redirect the user.

The present invention, through its use of client-side and server-side programs, allows for inter-domain cookie
10 access and analysis in order to provide enhanced functionality. This functionality may be extremely beneficial in the marketing, vendor control, online security, and online sales arena. In addition, the present invention may save time and valuable bandwidth, especially
15 for users receiving excessive or repetitive Internet advertisements, solicitations, or offers.

2. The Application is Ready for Allowance

None of the references cited by the Examiner teach or suggest a system for redirecting a user from a second
25 website to a first website if a determination is made that the user already possesses a product or has already

subscribed to a service via an analysis of cookie data.

The present invention reads cookie data, which is stored on a user's machine and perhaps created by another website, to make this determination. As discussed *supra* in section

5 "VII. **Arguments**" such an invention is fully described in the subject application so as to enable a person of ordinary skill to make or use the invention without undue experimentation. Thus, Appellant respectfully submits that the present application is ready for allowance. Early and
10 favorable consideration is appreciated.

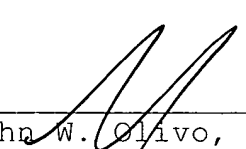
15

Respectfully submitted,

20

Date: May 31, 2005

25



John W. Olivo, Jr.
Reg. No. 35,634
WARD & OLIVO
382 Springfield Avenue
Summit, New Jersey 07901
(908) 277-3333

APPENDIX I: CLAIMS LISTING

5 1. (PREVIOUSLY PRESENTED) A method for redirecting a user
from a second Web site to a first Web site, comprising the
steps of:

- (1) providing, by the second Web site, a URL offering
a product or service to the user, said URL
10 specifying a program on the second Web site;
- (2) reading, by said program, a cookie located in the
user's computer in response to the user
activating said URL;
- (3) providing a positive determination when an
15 inquiry by said program, from said cookie as
to whether the user already possesses said
product or service is true;
- (4) redirecting, by said program, the user to the
first Web site when the determination of
20 step (3) is positive determination, wherein
the first Web site is specified by said
cookie; and
- (5) offering, by the second Web site, to supply said
product or service to the user when the
25 determination of step (3) is negative;

whereby the user who already possesses said
product or service will not receive
duplicate offers to supply said product or
service from multiple Web sites.

5 2. (ORIGINAL) The method of claim 1, wherein said
providing of step (1) comprises at least one of the
following steps of:

sending an e-mail including a link to said URL to
the user;

10 providing a Web page including a link to said URL
to the user; and

providing a computer program including a link to
said URL to the user.

3. (ORIGINAL) The method of claim 2, wherein said
15 activating of step (2) comprises at least one of the steps
of:

clicking a link to said URL on a Web page;

clicking a link to said URL in an e-mail; and

executing a computer program that activates a

20 link to said URL.

4. (ORIGINAL) The method of claim 1, further comprising a
step of:

placing, by the first Web site, said cookie the
user's computer in response to the user
registering with the first Web site for said
product or service, said cookie including
5 the URL of the first Web site.

5. (ORIGINAL) The method of claim 1, wherein said program
is a server side program.

6. (ORIGINAL) The method of claim 5, wherein said program
is at least one of the following:

10 a CGI script;
a Java servlet;
a PHP script; and
a Perl script.

7. (ORIGINAL) The method of claim 1, wherein said program
15 is a client side program that is downloaded from the second
Web site.

8. (ORIGINAL) The method of claim 7, wherein said program
is at least one of the following:

a Java applet;
20 a Java script; and
an Active X control.

9. (PREVIOUSLY PRESENTED) A system for re-directing a user
from a second Web site to a first Web site, comprising:

means for providing, in the second Web site, a
URL offering a product or service to the
user, said URL specifying a program on the
second Web site;

5 means for reading, in said program, a cookie
located on the user's computer in response
to the user activating said URL;

means for redirecting, in said program, the user
to the first Web site when the result of
10 said determining means is positive
determination, wherein the first Web site is
specified by said cookie; and

means for offering, in the second Web site, to
supply said product or service to the user
15 when the result of said determining means is
negative;

whereby the user who already possesses said
product or service will not receive
duplicate offers to supply said product or
20 service from multiple Web sites.

10. (ORIGINAL) The system of claim 9, wherein said
providing means comprises at least one of:

means for sending an e-mail including a link to
said URL to the user;

means for providing a Web page including a link
to said URL to the user; and

5 means for providing a computer program including
a link to said URL to the user.

11. (ORIGINAL) The system of claim 10, wherein said
activating of said URL comprises at least one of:

clicking a link to said URL on a Web page;

10 clicking a link to said URL in an-email; and

executing a computer program that activates a
link to said URL.

12. (PREVIOUSLY PRESENTED) The system of claim 9, further
comprising:

15 means for placing, in the first Web site, said
cookie on the user's computer in response to
the user registering with the first Web site
for said product or service, said cookie
including the URL of the first Web site.

20 13. (ORIGINAL) The system of claim 9, wherein said program
is a server side program.

14. (ORIGINAL) The system of claim 13, wherein said
program is at least one of the following:

a CGI script;
a Java servlet;
a PHP script; and
a Perl script.

5 15. (ORIGINAL) The system of claim 9, wherein said program
is a client side program that is downloaded from the second
Web site.

16. (ORIGINAL) The system of claim 15, wherein said
program is at least one of the following:

10 a Java applet;
a Java script; and
an Active X control.

17. (PREVIOUSLY PRESENTED) A computer program product
comprising a computer usable medium having control logic
15 stored therein for causing a computer to re-direct a user
from a second Web site to a first Web site, said control
logic comprising:

first computer readable program code means for
causing the computer to provide a URL
20 offering a product or service to the user;
second computer readable program code means for
causing the computer to read a cookie
located on the user's computer in response
to the user activating said URL;

third computer readable program code means for
causing the computer to provide a positive
determination in response to an inquiry from
said cookie as to whether the user already
5 possesses said product or service is true;

fourth computer readable program code means for
causing the computer to redirect the user to
the first Web site when the result of said
third means is a positive determination,
10 wherein the first Web site is specified by
said cookie; and

fifth computer readable program code means for
causing the computer to offer to supply said
product or service to the user when the
15 result of said third means is negative;

whereby the user who already possesses said
product or service will not receive
duplicate offers to supply said product or
service from multiple Web sites.

20 18. (ORIGINAL) The computer program of claim 17, wherein
said first means comprises at least one of:

computer readable program code means for causing
the computer to send an e-mail including a
link to said URL to the user;

computer readable program code means for causing
the computer to provide a Web page including
a link to said URL to the user; and

computer readable code means for causing the
computer to provide a computer program
including a link to said URL to the user.

5

APPENDIX II: EVIDENCE

APPENDIX II. A.

02-27-2002



101994351

documents or copy thereof:

1. Name of conveying party(ies):

HearMe, Inc.

2/11/02

Additional name(s) of conveying party(ies) attached?

☐ Yes

☐ No

3. Nature of Conveyance:

☒ Assignment

☐ Merger

☐ Security Agreement

☐ Change of Name

☐ Other:

Execution Date: December 19, 2001

2. Name and address of receiving party(ies):

Name: PalTalk Holdings, Inc.

Internal Address:

Street Address: 213 West 35th Street, 13th Floor

City: New York

State: NY Zip: 10001

Additional name(s) & address(es) attached?

☐ Yes

☐ No

4. Application number(s) or patent number(s):

If this document is being filed together with a new application, the execution date of the application is:

A. Patent Application No.(s): 09/542,090; 09/794,391;

09/768,320; 09/604,961; 09/248,371; 60/266,854; 09/614,867;
09/737,583

B. Patent No.(s):

Additional numbers attached? ☐ Yes ☒ No

5. Name and address of party to whom correspondence concerning document should be mailed:

Name: Rajiv P. Patel, Esq.

Internal Address: Fenwick & West LLP

Street Address: Two Palo Alto Square

City: Palo Alto State: CA Zip Code: 94306

6. Total number of applications involved: [8]

7. Total fee (37 CFR 3.41): \$320.00

☒ Check Enclosed

☐ Fee Transmittal Enclosed

☒ Charge any additional fees to the below mentioned deposit account.

8. Deposit Account No.: 19-2555

02/15/2002 BYTONE 00000104 09342079
09/FC/SAL 320.00 UP

DO NOT USE THIS SPACE

9. Statement and signature:

To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.

Rajiv P. Patel, Reg. 39,327

Name of Person Signing

Rajiv Patel

Signature

1/18/2002

Date

Total number of pages including cover sheet, attachments, documents: [2]

Mail documents to be recorded with required cover sheet information to: Box Assignment, Commissioner For Patents and Trademarks, Washington, D.C. 20231

Case Docket No.: 23014-01000

RIP / S. KRAUSE

23014/01000/DOCS/1238811.

PATENT
REEL: 012602 FRAME: 0230

CONFIRMATORY ASSIGNMENT OF PATENT APPLICATIONS

WHEREAS, We, the undersigned, whose business address is set forth below, have owned and/or acquired certain rights in the inventions as set forth in the specifications and claims of United States Patent Application Serial Nos. 09/542,090; 09/794,391; 09/768,320; 09/604,961; 09/248,371; 60/266,854; 09/614,867; and 09/737,583.

WHEREAS, PalTalk Holdings, Inc., a Delaware Corporation having a place of business at 213 West 35th Street, Thirteenth Floor, New York, NY 10001 (hereinafter referred to as ASSIGNEE), is desirous of acquiring the entire interest in, to and under said inventions and in, to and under said United States Patent Application Serial Nos. 09/542,090; 09/794,391; 09/768,320; 09/604,961; 09/248,371; 60/266,854; 09/614,867; and 09/737,583 or any Letters Patent or similar legal protection to be obtained therefore in the United States and in any and all foreign countries.

NOW, THEREFORE, TO ALL WHOM IT MAY CONCERN, be it known that for good and valuable consideration, We hereby sell, assign and transfer to ASSIGNEE the full and exclusive right, title and interest in and to said inventions in the United States and its territorial possessions, and in all foreign countries, and to said United States Patent Application Nos. 09/542,090; 09/794,391; 09/768,320; 09/604,961; 09/248,371; 60/266,854; 09/614,867; and 09/737,583, and to all Letters Patent or similar legal protection in the United States and its territorial possessions, and in any and all foreign countries, to be obtained for said inventions, or any continuation, divisional, renewal, substitute or reissue thereof or any legal equivalent thereof in a foreign country or the full term or terms for which the same may be granted.

We HEREBY COVENANT that no assignment, sale, agreement or encumbrance has been or will be made or entered into which would conflict with this assignment and sale; and

IN WITNESS WHEREOF, We have hereunto set hand and seal this 19th day of December, 2001.

HearMe,

By:

Signature:

Name Printed:

Title:

James R. Schmidt
CEO James R. Schmidt
CEO 19-DEC-2001 15150

Post Office Address: HearMe, Inc.
685 Clyde Avenue
Mountain View, CA 94043

APPENDIX II. B.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Sahai et al.

Serial No.: 09/614,867

Examiner: Chad Zhong

Filed: 7/12/2000

Group Art Unit: 2154

For: METHOD AND COMPUTER PROGRAM PRODUCT FOR WEB SITE
USER REDIRECTION

AMENDMENT AND RESPONSE

Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

Dear Sir:

In response to the Office Action dated October 6, 2003 (the "Office Action"), Applicants respectfully request continued examination in the application and entry of the following amendment to the above-identified case as follows:

Petition for Extension of Time. Applicant herewith petitions for a **Three-month** extension of time to respond to the above-identified office action. In the event that an extension of time is required and applicant has inadvertently overlooked the need to petition for such extension, the applicant hereby petitions for such extension of time.

Fees. The Commissioner is hereby authorized to charge the following fees to Skadden Arps' deposit account **19-2385**:

\$940 fee for three-month extension;

Any additional fees required in connection with this submission or any required petition.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for re-directing a user from a second Web site to a first Web site, comprising the steps of:

- (1) providing, by the second Web site, a URL offering a product or service to the user, said URL specifying a program on the second Web site;
- (2) reading, by said program, a cookie located in the user's computer in response to the user activating said URL;
- (3) providing a positive determination when an inquiry determining, by said program, from said cookie as to whether the user already possesses said product or service is true;
- (4) redirecting, by said program, the user to the first Web site when the determination of step (3) is positive determination, wherein the first Web site is specified by said cookie; and
- (5) offering, by the second Web site, to supply said product or service to the user when the determination of step (3) is negative;

whereby the user who already possesses said product or service will not receive duplicate offers to supply said product or service from multiple Web sites.

2. (original) The method of claim 1, wherein said providing of step (1) comprises at least one of the steps of:

sending an e-mail including a link to said URL to the user;

providing a Web page including a link to said URL to the user; and

providing a computer program including a link to said URL to the user.

3. (original) The method of claim 2, wherein said activating of step (2) comprises at least one of the steps of:

clicking a link to said URL on a Web page;

clicking a link to said URL in an e-mail; and

executing a computer program that activates a link to said URL.

4. (original) The method of claim 1, further comprising a step of:

placing, by the first Web site, said cookie on the user's computer in response to the user registering with the first Web site for said product or service, said cookie including the URL of the first Web site.

5. (original) The method of claim 1, wherein said program is a server side program.

6. (original) The method of claim 5, wherein said program is at least one of the following:

a CGI script;

a Java servlet;

a PHP script; and

a Perl script.

7. (original) The method of claim 1, wherein said program is a client side program that is downloaded from the second Web site.

8. (original) The method of claim 7, wherein said program is at least one of the following;

a Java applet;

a Java script; and

an Active X control.

9. (currently amended) A system for re-directing a user from a second Web site to a first Web site, comprising:

means for providing, in the second Web site, a URL offering a product or service to the user, said URL specifying a program on the second Web site;

means for reading, in said program, a cookie located on the user's computer in response to the user activating said URL;

means for providing a positive determination when an inquiry determining, in said program, from said cookie as to whether the user already possesses said product or service is true;

means for redirecting, in said program, the user to the first Web site when the result of said determining means is positive determination, wherein the first Web site is specified by said cookie; and

means for offering, in the second Web site, to supply said product or service to the user when the result of said determining means is negative;

whereby the user who already possesses said product or service will not receive duplicate offers to supply said product or service from multiple Web sites.

10. (original) The system of claim 9, wherein said providing means comprises at least one of:

means for sending an e-mail including a link to said URL to the user;

means for providing a Web page including a link to said URL to the user;

and

means for providing a computer program including a link said URL to the user.

11. (original) The system of claim 10, wherein said activating of said URL comprises at least one of:

clicking a link to said URL on a Web page;

clicking a link to said URL in an e-mail; and

executing a computer program that activates a link to said URL.

12. (original) The system of claim 9, further comprising:

means for placing, in the first Web site, said cookie on the user's computer in response to the user registering with the first Web site for said product or service, said cookie including the URL of the first Web site.

13. (original) The system of claim 9, wherein said program is a server side program.

14. (original) The system of claim 13, wherein said program is at least one of the following:

a CGI script;

a Java servlet;

a PHP script; and

a Perl script.

15. (original) The system of claim 9, wherein said program is a client side program that is downloaded from the second Web site.

16. (original) The system of claim 15, wherein said program of is at least one of the following:

a Java applet;

a Java script; and

an Active X control.

17. (currently amended) A computer program product comprising a computer usable medium having control logic stored therein for causing a computer to re-direct a user from a second Web site to a first Web site, said control logic comprising:

first computer readable program code means for causing the computer to provide a URL offering a product or service to the user;

second computer readable program code means for causing the computer to read a cookie located on the user's computer in response to the user activating said URL;

third computer readable program code means for causing the computer to provide a positive determination in response to an inquiry determine from said cookie as to whether the user already possesses said product or service is true;

fourth computer readable program code means for causing the computer to redirect the user to the first Web site when the result of said third means is positive determination, wherein the first Web site is specified by said cookie; and

fifth computer readable program code means for causing the computer to offer to supply said product or service to the user when the result of said third means is negative;

whereby the user who already possesses said product or service will not receive duplicate offers to supply said product or service from multiple Web sites.

18. (original) The computer program product of claim 17, wherein said first means comprises at least one of:

computer readable program code means for causing the computer to send an e-mail including a link to said URL to the user;

computer readable program code means for causing the computer to provide a Web page including a link to said URL to the user; and

computer readable program code means for causing the computer to provide a computer program including a link to said URL to the user.

REMARKS

Claims 1-18 are pending in this Application. Claim 1-18 stand rejected under 35 U.S.C. § 112, first paragraph. Claims 1, 9, and 17 stand rejected under 35 U.S.C. § 112 second paragraph. Claims 1, 9, and 17 have been amended. Applicants respectfully request reconsideration of the pending claims 1-18 in light of the amendments following remarks.

Rejection of Claims 1-18 under 35 U.S.C. § 112

The Office Action rejected Claims 1-18 under 35 U.S.C. § 112, first paragraph as failing to comply with the enablement requirement. Specifically, The Office Action stated that the claims fail to disclose how a second website program will read a cookie place by a first site program since cookie programs from a first domain cannot read cookies from a second domain. Applicants disagree with the Office Action that cookies cannot be read by a domain that did not place the cookies. Specifically, the Office Action provided an article about cookies from Sentrysystems.com that discusses the fact that cookies can indeed be read between different domains: "Most companies now encrypt cookies. That is, they scramble the cookie so that only the server or application that created the cookie can decipher the contents of the cookie." (Printed Page 2) Hence, when cookies are not encrypted, any domain is able to read their content, since they are merely text files, as discussed on the Sentrysystems.com article. Accordingly, applicants submit that Claims 1-18 comply with 35 U.S.C. § 112, first paragraph by describing a cookie placed by a first domain.

The Office Action further rejected Claims 1, 9, and 17 under 35 U.S.C. § 112, second paragraph as being indefinite. Applicants have amended Claims 1, 9, and 17 to more clearly recite that "positive" means "true" and "negative" means "false." Accordingly, Claims 1, 9, and 17 are in compliance with 35 U.S.C. § 112, second paragraph.

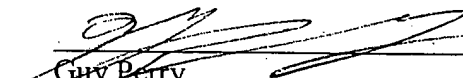
SUMMARY

Applicants have amended the claims to overcome the 35 U.S.C. § 112 rejections. In view of the forgoing supporting remarks and amendments, Applicants respectfully request allowance of pending claims 1-18.

If the Examiner wishes to direct any questions concerning this application to the undersigned Applicants' representative, please call the number indicated below.

Dated: April 5, 2004

Respectfully submitted,


Guy Perry
Reg. No. 46,194

Attorney for Applicants
(212) 735-3000
Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036

APPENDIX II. C.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,867	07/12/2000	Shankar Sahai	1719.0360000	2450

7590

04/29/2004

ADREW F. STROBERT
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
FOUR TIMES SQUARE
NEW YORK, NY 10036

EXAMINER

ZHONG, CHAD

ART UNIT

PAPER NUMBER

2154

DATE MAILED: 04/29/2004

8

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary

Application No.

09/614,867

Applicant(s)

SAHAI ET AL.

Examiner

Chad Zhong

Art Unit

2154

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☒ Claim(s) 1,9 and 17 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

Final Action

1. This action is responsive to communications: Amendment, filed on 04/07/2004. This action has been made final.
2. Claims 1-18 are presented for examination. In amendment A, filed on 04/07/2004: claims 1, 9, 17 are amended.
3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention of which the claims are directed. The current title is imprecise.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.
5. Claims 1-18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Applicants fail to teach the detail of reading the cookie residing in a client computer and to take different courses of actions depending upon the content of the cookie. Specifically, Applicants fail to teach the special steps taken by a second website's program to read the cookie stored in the user's computer and to determine the content of

Art Unit: 2154

the cookie.

According to the specification of the Persistent Client State HTTP Cookies¹ program from a second domain cannot read cookie from a first domain. "A cookie can only be read and modified by an object in the valid domain and path defined in the cookie when it was created. The domain path cannot be set to send cookies to a domain outside of the domain where server creating the cookie resides. The domain attribute is set to the domain of the document sending the cookie by default"².

If a cookie contains information indicating that the user's computer has already installed a product related to the first website, the cookie inherently is set by the first website. If the second website is going to offer the user a product when the user has not already used the product from the first website, the second website inherently is different and distinct from the first website, i.e. the two websites have different domains.

In order to implement the claimed invention, it requires the program from the second domain [second website] to read the cookie from the first domain [first website]. However, according to the specification of HTTP Cookies as set forth hereinabove, no other website [the second website] can read the first website's cookie. As such, it is not clear how the claimed invention can be implemented while still following the specification of the HTTP Cookies. In summary, applicants fail to teach the specific methods which allow the program in the second website to read the first website's cookie stored in the user's computer.

The Examiner submits that it would require undue experimentation for one of ordinary skill in the art to make and use the invention for the reason set forth

Art Unit: 2154

hereinabove. Applicants are reminded that no new matter is allowed in the amendment to the specification under 35 U.S.C 132 and 37 CFR 1.118(a).

¹ [Http://wp.setscape.com/newsref/std/cookie_spec](http://wp.setscape.com/newsref/std/cookie_spec)

² [Http://webmaster.info.aol.com/aboutcookies](http://webmaster.info.aol.com/aboutcookies)

6. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. The claim language in the following claims is murky or not clearly understood:

i. As per claim 1, line 11, it is not clearly understood the meaning of the word "positive" (i.e. does positive mean true when determination from cookie whether the user already possesses product or service?); line 14, it is not clearly understood the meaning of the word "negative" (i.e. does negative mean false when determination from cookie whether the user already possesses product or service?).

ii. As per claim 9, line 11, it is not clearly understood the meaning of the word "positive" (i.e. does positive mean true when determination from cookie whether the user already possesses product or service?); line 14, it is not clearly understood the meaning of the word "negative" (i.e. does negative mean false when determination from cookie whether the user already possesses product or service?).

iii. As per claim 17, line 14, it is not clearly understood the meaning

of the word "positive" (i.e. does positive mean true when determination

from cookie whether the user already possesses product or service?); line 17, it is not clearly understood the meaning of the word “negative” (i.e. does negative mean false when determination from cookie whether the user already possesses product or service?).

Conclusion

14. Applicant's remarks filed 04/07/2004 have been considered but are found not persuasive in view at the new grounds at rejection necessitated by Applicant's amendment.

15. In the remark, the applicant argued in substance that there exist system wherein cookies can indeed be read between different domains and cited specific sections on page 2 of Sentrysystems.com as evidence. The applicant further went on to explain the encryption of cookies by companies allows only server or application that created the cookie can decipher the contents of the cookie, accordingly without encryption, cookies can be read across different domains.

In response to applicant's amendment, the Sentrysystems.com paper provide further evidence that cookies can not be shared across different domains. Referring to page 2 and 3, under section “What Can Cookies NOT Do?”, there exist a subsection “Cookies can not be transferred to other domains”. This sections explicitly states that “it is impossible to send cookie information other domains for systems adhering to the cookie specification”. The special case being “cookie replication service”, of which Sentrysystem.com does not provide. Thus, Sentrysystem.com does not teach sharing of cookies across different domains as it is impossible.

THIS ACTION IS MADE FINAL. Applicant is reined of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following patents and publications are cited to further show the state of the art with respect to changing program of remote nodes.

- i. US 6/064,979 to Perkowski. Discloses e-commerce application comparing different product numbers to determine the availability of the service. compare UPN against MIN
- ii. US 6/035,334 to Martin et al. Teaches redirection and URL embedded within the cookie.
- iii. US 2002/0019828 to Mortl. Teaches redirection and URL embedded within the cookie.
- iv. US 2002/0035611 to Dooley. Teaches redirection and URL embedded within the cookie.
- v. US 6/161,643 to Cheng et al. Teaches software updates different vendors.
- vi. US 2002/0099622 to Langhammer. Teaches cookie checking in E-commerce environment
- vii. US 2002/0062343 to Appleman et al. Teaches redirection and URL embedded within the cookie. URL, redirection, cookies.

Art Unit: 2154

- viii. US 6/453347 to Revashetti et al. Teaches determining by program from cookie whether the user already possesses product or service, the offering by the website to supply product or service to the user when determination of availability of the product or service is negative.
- ix. US 2002-0199004 to Jaye. Teaches a site provide URL offering product/service as well as specifying a program on the site, next redirection of user is possible based on URL provided in the cookie.
- xi. Telecommunications system. St. Louis: Jun 1997. Vol. 69, Iss. 6; pg 8, 2 Cookies on your hard drive. Wayland Hancock Teaches cookies on local harddrive and their impacts to the user and network environment.
- xii. Cookiecentral.com "The dark side", teaches cookies issued by the same server can be read later by the same server
- xiii. "Persistent Client State HTTP Cookies", disclosed only host within the specified domain can set a cookie on domain.
- xiv. "Microsoft Cookies jump Domains", teaches direct to server which controls globally unique identifiers (GUIDs)
- xv. AOL Webmaster.info, "About Cookies", disclosed that a cookie can be accessed only by another server/host from the same domain, wherein the server is the one who creates the cookie.
- xvi. Internet Explorer "Open Cookie Jar", disclose how a web site can read Internet Explorer (IE) cookies set from ANY domain by redirect and **mislead** the IE to read the cookie in the other domain.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chad Zhong whose telephone number is (703)305-0718. The examiner can normally be reached on M-F 7:15 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng An can be reached on (703)305-9678. The fax phone numbers for the

Art Unit: 2154

organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-872-9306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

CZ

April 19, 2004

A handwritten signature in black ink, appearing to be 'JF', is centered on the page.

**JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100**

APPENDIX II. D.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Shankar Sahai et al.

Serial No.: 09/614,867

Group Art Unit: 2154

Filed: 7/12/2000

Examiner: Chad Zhong

Atty. Doc. No.: 630-015

For: METHOD AND COMPUTER PROGRAM FOR WEB SITE USER
REDIRECTION

Honorable Commission of Patents and Trademarks
Washington, DC. 20231

RESPONSE TO OFFICE ACTION

S I R:

In response to the April 19, 2004 Office Action in the
above mentioned case, Applicants respectfully request
reconsideration in view of the following amendments and
remarks as follows:

Amendments to the Specification begin on page 3 of this
paper.

Amendments to the Claims begin on page 4 of this paper.

Remarks/Arguments begin on page 11 of this paper.

Petition for Extension of Time. Applicants herewith petition for a **Three-month** extension of time to respond to the above-identified office action.

5

AMENDMENTS TO THE SPECIFICATION

Please amend the specification as follows:

Applicants submit the following title for the invention:

5 ~~METHOD AND COMPUTER PROGRAM FOR WEB SITE USER~~
~~REDIRECTION~~

METHOD AND COMPUTER PROGRAM FOR OFFERING PRODUCTS AND
SERVICES BY EXAMINING USER ACTIONS

AMENDMENTS TO THE CLAIMS

1. (CURRENTLY AMENDED) A method for redirecting a user from a second Web site to a first Web site, comprising the steps of:

5 (1) providing, by the second Web site, a URL offering a product or service to the user, said URL specifying a program on the second Web site;

 (2) reading, by said program, a ~~cookie~~ block of data located in the user's computer in response to the user
10 activating said URL;

 (3) providing a positive ~~determination~~ indication when an inquiry by said program, ~~from~~ to said ~~cookie~~ block of data ~~as to whether the~~ determines that the user already possesses said product or service ~~is true~~;

15 (4) redirecting, by said program, the user to the first Web site when the ~~determination~~ indication of step (3) is positive ~~determination~~, wherein the first Web site is specified by said ~~cookie~~ block of data; and

 (5) offering, by the second Web site, to supply said
20 product or service to the user when the ~~determination~~ indication of step (3) is ~~negative~~ not positive;

whereby the user who already possesses said product or service will not receive duplicate offers to supply said product or service from multiple Web sites.

2. (ORIGINAL) The method of claim 1, wherein said providing of step (1) comprises at least one of the following steps of:

5 sending an e-mail including a link to said URL to the user;

providing a Web page including a link to said URL to the user; and

providing a computer program including a link to said URL to the user.

10 3. (ORIGINAL) The method of claim 2, wherein said activating of step (2) comprises at least one of the steps of:

clicking a link to said URL on a Web page;

clicking a link to said URL in an e-mail; and

15 executing a computer program that activates a link to said URL.

4. (CURRENTLY AMENDED) The method of claim 1, further comprising a step of:

placing, by the first Web site, said ~~cookie~~ block of
20 data on the user's computer in response to the user registering with the first Web site for said product or service, said ~~cookie~~ block of data including the URL of the first Web site.

5. (ORIGINAL) The method of claim 1, wherein said program is a server side program.

6. (ORIGINAL) The method of claim 5, wherein said program is at least one of the following:

- 5 a CGI script;
- a Java servlet;
- a PHP script; and
- a Perl script.

7. (ORIGINAL) The method of claim 1, wherein said program
10 is a client side program that is downloaded from the second Web site.

8. (ORIGINAL) The method of claim 7, wherein said program is at least one of the following:

- a Java applet;
- 15 a Java script; and
- an Active X control.

9. (CURRENTLY AMENDED) A system for re-directing a user from a second Web site to a first Web site, comprising:

means for providing, in the second Web site, a URL
20 offering a product or service to the user, said URL specifying a program on the second Web site;

means for reading, in said program, a ~~cookie~~ block of data located on the user's computer in response to the user activating said URL;

means for redirecting, in said program, the user to the first Web site when the result of said ~~determining~~ indication means is positive ~~determination~~, wherein the first Web site is specified by said ~~cookie~~ block of data;

5 and

means for offering, in the second Web site, to supply said product or service to the user when the result of said ~~determining~~ indication means is ~~negative~~ not positive;

whereby the user who already possesses said product or
10 service will not receive duplicate offers to supply said product or service from multiple Web sites.

10. (CURRENTLY AMENDED) The system of claim 9, wherein said providing means comprises at least one of:

means for sending an e-mail including a link to said
15 URL to the user;

means for providing a Web page including a link to said URL to the user; and

means for providing a computer program including a link to said URL to the user.

20 11. (ORIGINAL) The system of claim 10, wherein said activating of said URL comprises at least one of:

clicking a link to said URL on a Web page;

clicking a link to said URL in an-email; and

executing a computer program that activates a link to said URL.

12. (CURRENTLY AMENDED) The system of claim 9, further comprising:

5 means for placing, in the first Web site, said ~~cookie~~ block of data on the user's computer in response to the user registering with the first Web site for said product or service, said ~~cookie~~ block of data including the URL of the first Web site.

10 13. (ORIGINAL) The system of claim 9, wherein said program is a server side program.

14. (ORIGINAL) The system of claim 13, wherein said program is at least one of the following:

a CGI script;
15 a Java servlet;
a PHP script; and
a Perl script.

15. (ORIGINAL) The system of claim 9, wherein said program is a client side program that is downloaded from the second
20 Web site.

16. (ORIGINAL) The system of claim 15, wherein said program is at least one of the following:

a Java applet;
a Java script; and

an Active X control.

17. (CURRENTLY AMENDED) A computer program product comprising a computer usable medium having control logic stored therein for causing a computer to re-direct a user
5 from a second Web site to a first Web site, said control logic comprising:

first computer readable program code means for causing the computer to provide a URL offering a product or service to the user;

10 second computer readable program code means for causing the computer to read a ~~cookie~~ block of data located on the user's computer in response to the user activating said URL;

third computer readable program code means for causing
15 the computer to provide a positive ~~determination~~ indication in response to an inquiry ~~from~~ to said ~~cookie~~ block of data as to whether the user already possesses said product or service ~~is true~~ when the user does already possess said product or service;

20 fourth computer readable program code means for causing the computer to redirect the user to the first Web site when the result of said third means is a positive ~~determination~~ indication, wherein the first Web site is specified by said ~~cookie~~ block of data; and

fifth computer readable program code means for causing the computer to offer to supply said product or service to the user when the result of said third means is ~~negative~~ not a positive indication;

5 whereby the user who already possesses said product or service will not receive duplicate offers to supply said product or service from multiple Web sites.

18. (ORIGINAL) The computer program of claim 17, wherein said first means comprises at least one of:

10 computer readable program code means for causing the computer to send an e-mail including a link to said URL to the user;

 computer readable program code means for causing the computer to provide a Web page including a link to said URL
15 to the user; and

 computer readable code means for causing the computer to provide a computer program including a link to said URL to the user.

REMARKS

Applicants have amended claims 1-18 to overcome the objection that they fail to comply with the enablement requirement. Claims 1-18 have been amended to no longer
5 use cookies in a fashion that they are currently not capable of performing. Furthermore, Applicants have also amended claims 1, 9 and 17 to overcome the indefinite objection by the Examiner for failing to particularly point out and distinctly claim the subject matter which the
10 Applicants regard as the invention. Claims 1, 9 and 17 now clearly detail what a positive indication means. In addition, the Examiner has objected to the title of the invention for being imprecise. Applicants have amended the title of the invention to clearly indicate the invention of
15 which the claims are directed. Applicants believe that the forgoing amendments and the comments that follow will convince the Examiner that the rejections and objections in the April 19, 2004 Office Action have been overcome and should be withdrawn.

I. **THE EXAMINER'S OBJECTIONS**

The Examiner objected to claims 1, 9, and 17 under 35 U.S.C. §112, second paragraph as being indefinite. The Examiner states that these are unclear in the meaning of
5 the words "positive" and "negative" as used in the claims.

II. **THE EXAMINER'S REJECTIONS**

The Examiner rejected claims 1-18 under 35 U.S.C § 112, first paragraph as failing to comply with the enablement requirement. The Examiner stated that the
10 applicants fail to teach

"the detail of reading the cookie residing in a client computer and to take different courses of action depending on the content of the cookie. Specifically, Applicants fail to teach the special steps taken by a
15 second website's program to read the cookie stored in the user's computer and to determine the content of the cookie."

The Examiner bases this objection on the argument that
20 cookies "can only be read and modified by an object in the valid domain and path defined in the cookie when it was created."

III. **THE EXAMINER'S OBJECTION TO THE SPECIFICATION**

The Examiner has objected to the title of the
25 invention for being imprecise. The Examiner states that the title fails to clearly indicate "the invention to which the claim are directed."

IV. THE EXAMINER'S OBJECTIONS AND REJECTIONS SHOULD BE
WITHDRAWN

A. CLAIM OBJECTIONS

5 The Applicants respectfully submit that the Examiner's
objections should be withdrawn in view of the foregoing
amendments to independent claims 1, 9, and 17. The Office
Action states that as previously written claims 1, 9 and 17
are unclear as to what is meant by "positive" and
10 "negative" determinations. Specifically, the Examiner
states the claims are unclear as to if "positive" and
"negative" refer to whether the user already possesses the
product or service. To clarify what is meant, Applicants
have removed reference to positive and negative
15 determinations and replaced them with a "positive
indication." A positive indication, as detailed in the
claims, indicates that a user does already possess the
product or service being checked. When the indication is
not "positive" (i.e., it has not determined positively that
20 the user possesses the product or service being checked)
the user is then offered the product or service.

B. CLAIM REJECTIONS

The Office Action rejected claims 1-18 under 35 U.S.C
§ 112, first paragraph as failing to comply with the
25 enablement requirement. The Examiner supports this

objection by arguing that by design cookies can only be read and modified by a Web site falling under the domain that first created them. Applicants agree with the Examiner that as currently designed cookies can only be
5 read and modified by the Web Site that first created the cookie. To overcome this limitation, claims 1-18 have been amended to use "blocks of data" in a unique fashion. These "blocks of data" function in much the same way as cookies yet unlike cookies are not limited to being read and
10 modified only by the Web Site that first created them. Applicants argue that creating and implementing these "blocks of data" would be obvious to one skilled in the relevant arts. The purpose of these files would be similar to cookies, except they would be sharable. These files
15 could be used in conjunction with cookies as they are currently designed or they could represent future designs of cookies that are sharable or at least partly sharable.

C. REJECTION OF TITLE

The Office Action has objected to the title of the
20 invention for failing to clearly indicate the invention to which the claims are directed. Applicants have submitted a new title to overcome this objection.

In light of the foregoing amendments and remarks, applicants submit that the present application is now in condition for allowance. No new matter has been added.

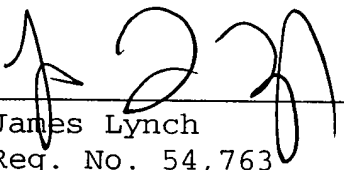
CONCLUSION

Applicants submit that all pending claims represent a patentable contribution to the art and are in condition for allowance. Early and favorable action is accordingly
5 solicited.

Respectfully submitted,

10

Date: 10-29-04


James Lynch
Reg. No. 54,763
Ward & Olivo
382 Springfield Ave.
Summit, NJ 07901
908-277-3333

APPENDIX II. E.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,867	07/12/2000	Shankar Sahai	1719.0360000	2450

7590 02/14/2005
JOHN W. OLIVO, JR.
WARD & OLIVO
382 SPRINGFIELD AVENUE
SUMMIT, NJ 07901

EXAMINER

ZHONG, CHAD

ART UNIT	PAPER NUMBER
----------	--------------

2152

DATE MAILED: 02/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

09/614,867

Applicant(s)

SAHAI ET AL.

Examiner

Chad Zhong

Art Unit

2152

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 01 November 2004 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☒ The reply was filed after the date of filing a Notice of Appeal, but prior to the date of filing an appeal brief. The Notice of Appeal was filed on 01 November 2004. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____

Claim(s) objected to: _____

Claim(s) rejected: 1-18.

Claim(s) withdrawn from consideration: _____

AFFIDAVIT OR OTHER EVIDENCE

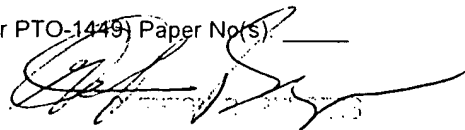
8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____

12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s): _____

13. ☐ Other: _____


CHAD ZHONG
2152

Continuation of 3. NOTE: while applicant amended the claims so as to replace the claimed "cookie" with ---block of data---, the amended does not overcome the 35 USC 112, 1st rejection (recited in the final office action, mailed 4/29/04). As stated in the final office action, page 3, third paragraph, applicants fail to teach the specific methods which allow the program in the second website to read the first website's cookie (or block of data) stored in the user's computer. It should be noted that such a method is not well known in the art.

Further, applicant's originally filed specification is not amended so as to contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same.

APPENDIX II. F.

[MSDN Home](#) > [MSDN Library](#) > [Win32 and COM Development](#) > [Component Development](#) > [ActiveX Controls](#) > [Overviews/Tutorials](#)

Designing Secure ActiveX Controls

[Internet Development Index](#)

Any Microsoft ActiveX control should be conceived and designed with security in mind.

An ActiveX control can be an extremely insecure way to provide a feature. Because it is a Component Object Model (COM) object, it can do anything the user can do from that computer. It can read from and write to the registry, and it has access to the local file system. From the moment a user downloads an ActiveX control, the control may be vulnerable to attack because any Web application on the Internet can repurpose it, that is, use the control for its own ends whether sincere or malicious. But, you can take precautions when you write a control to help avert an attack.

You have a responsibility to users to provide the most secure controls. Do not assume that your control is secure until it has gone through a rigorous security review. This article contains some guidelines you can incorporate into your security review process.

This article contains information about the following topics:

- [Security Considerations](#)
- [How to Judge Control Security](#)
- [Preventing Repurposing](#)
- [Related Topics](#)

Security Considerations

Designing for security is important because an ActiveX control is particularly vulnerable to attack. An application running on any Web site can use the control; all that it needs is the control's class identifier (CLSID). The control may be repurposed, that is, used in ways that you did not intend. The repurposing might be friendly or a malicious attack on the computer running the control. As you design a control, think about what specific measures you should take to protect it.

Before you implement a feature as an ActiveX control, consider whether you can achieve the same functionality through other means. If you do not need access to system resources, you can write the control as a [Dynamic HTML \(DHTML\) behavior](#).

Because an ActiveX control is a Microsoft Win32 component, there is no sandboxing, that is, it can run without restrictions. You should think about how you can restrict functionality to prevent others from repurposing your control to possibly malicious ends.

- Can the control be made to call other objects on the page, including Java applets? The Microsoft virtual machine (Microsoft VM) called from native code in the control might attribute greater permissions to the control than script on the page has. If the script can manipulate the control to call the Microsoft VM for it, an indirect security attack might be possible.
- Can the control tunnel out of the frame in which it is hosted and access content in another frame? The data accessed could potentially violate the privacy of the user. You might prevent this by restricting the control to run only within a particular domain.
- Many ActiveX controls are initialized with data from local or remote sites, and most ActiveX controls are scriptable (they support a set of methods, events, and properties). Both initialization of persisted data and use of the controls through scripting require safeguards to ensure that security is not violated. If your control does not read persisted data, don't mark it as safe for initialization. If your control is not designed for use in a browser, don't mark it as safe for scripting.

You should [digitally sign](#) every ActiveX control. Digital signing tells users where the control came from and verifies that the control has not been tampered with since its publication.

Be sure the control doesn't loop infinitely or stop responding when given bad data or arguments. An attacker might tie up a user's computer using your ActiveX control.

It is important for a secure ActiveX control to check all inputs and guard against buffer overrun. If a control receives an input string into a fixed-length buffer without checking its length first, it is possible for a malicious caller to provide a string that is longer than the allocated buffer, overwriting other information in an unintended way. In some cases, these bugs can be exploited to make the control perform unsafe operations it was not designed to do. As the author of an ActiveX control, you need to be vigilant. Never assume that a certain input conforms to certain requirements. Always check the data to avoid these attacks. All inputs should have maximum sizes, and controls should be tested to perform safely, even with inputs that are beyond specifications. See [Fix Those Buffer Overruns](#) for more information.

How to Judge Control Security

The following questions are designed to help you build a more secure ActiveX control. You can use them as part of your larger security review. Think about how to answer each question and how you might design your control more securely. The security of a control is ultimately a subjective judgment. As a general rule, if you answer yes to any of these questions you should probably not mark the control as safe for scripting or safe for data initialization, or you should implement some type of lock down security, that is, restrict the use of the control to within a specific set of domains.

- Can you limit domain usage or zone usage? See [Preventing Repurposing](#) for more information.
- Are you exposing the user's private information over the network or to other users?
- Can you read, write, create, detect or delete arbitrary persisted data either on the file system, the registry, a buddy list, or a camera or other USB devices?
- Does this control enable data to passing from one Internet site to another? From the intranet to the Internet? From the local computer to the Internet?
- Can this control host mobile code or script? If so, where does the code or script come from?
- Does the control cause arbitrary operations or programs to execute on behalf of the user without notice?
- Does this control circumvent/defeat a specific security feature in the browser, operating system, or another application?
- Can a Web page use this control to cause the system to become unstable or stop responding?
- Can this control be used to spy on the user without their knowledge?
- Is there a possibility for cross-site scripting attacks using this control?
- Does this control load its own data format? Does this data type have its own security implementation? Does this data type allow macros?
- Is history, statistical, or debugging information persisted on the local computer? Can a privacy conscious user clear this information? Is the information ever sent over the network? Are globally unique identifiers (GUIDs) used to track users?

These are some other general questions that you should consider as you design your control.

- Are strings from the network validated, parsed, or filtered? What happens with the strings? What would happen if they contain script? What happens to the strings after they are passed on to another component?
- Where might there be buffer overruns? Have you done full testing for buffer overruns on all methods, properties, and events?
- What are you doing to stop an extraneous Web site from invoking the control?
- If you don't mark the control "safe for scripting" or "safe for initialization", does that disable the purpose of the control? Controls are marked as not safe for scripting or data initialization by default. Don't implement them unless the functionality of the control is hampered without them.
- Does the control present information to the user such that they can always identify its authenticity? Do you digitally sign the control?

In addition, it is a good idea to document the following information about your control for reference.

- Methods
- Properties
- CLSID
- Events
- Owner

- [DLL/OCX name and version](#)

Preventing Repurposing

If you don't take precautions when you develop the control, an ActiveX control has virtually unlimited access to the computer it resides on. It can change registry settings, can manipulate the local file system, and can provide security rights not normally available to an external Web site. An attacker can repurpose an ActiveX control and use it to gain access to the computer.

Marking an ActiveX control as safe for scripting can leave you open to attack. Do not mark a control as safe for scripting unless you absolutely have to. You can use the list of questions in [How to Judge Control Security](#) while designing your control to help you decide.

If you decide that your control must be marked as safe for scripting, then you can protect the control by restricting the domains in which the control can be scripted. This is referred to as "locking down your control" and should make it harder for a control to be maliciously repurposed.

You can [download](#) and use the SiteLock template. This template includes instructions to help you write a secure control that restricts the domains in which it can be scripted.

Related Topics

- [Introduction to ActiveX Controls](#)
- [Safe Initialization and Scripting for ActiveX Controls](#)
- [Signing Code with Microsoft Authenticode Technology](#)
- [Introduction to URL Security Zones](#)
- [IObjectSafety](#)
- [Using ActiveX Controls to Automate Your Web Pages](#)

[Manage Your Profile](#) | [Legal](#) | [Contact Us](#) | [MSDN Flash Newsletter](#)

© 2005 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)



APPENDIX II. G.

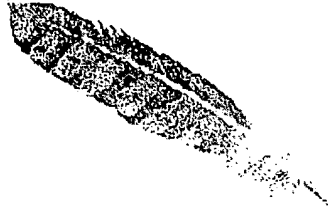
The Source

<http://java.sun.com/developer/technicalArticles/Security/Signed/>**Article****Signed Applets, Browsers, and File Access**

Articles Index

Monica Pawlan and Satya Dodda

April 1998



Have you ever asked yourself "How do I sign an applet so it can access local system resources?", or "Why does an applet work in Applet Viewer, but not in my browser?" This article answers these questions, and shows you how to sign an applet, give it access to a local file, and successfully run it.

By default, applets have no access to system resources outside the directory from which they were launched, but a signed applet can access local system resources as allowed by the local system's security policy. The Java Development Kit (JDK) 1.2 provides security tools so end users and system administrators can sign applets and applications, and define their local security policy by specifying in a policy file how

much access to local system resources a signed applet or application can have.

Web Browsers

A JDK 1.2 applet can run in a browser enabled for JDK 1.2 or in Applet Viewer. If an applet attempts to access local system resources, the applet must be signed and the local system must have a policy file configured to allow the access. If a JDK 1.2 applet does not work when you run it in your browser, it is probably because your browser is not enabled for JDK 1.2, or the applet is not signed, or you do not have a correctly configured policy file.

When Project Java Activator ports to JDK 1.2, you can upgrade operating systems and browsers to the latest Java platform at any time and independent of operating system or web browser upgrades. See the Project Java Activator page for more information.

Local File Access

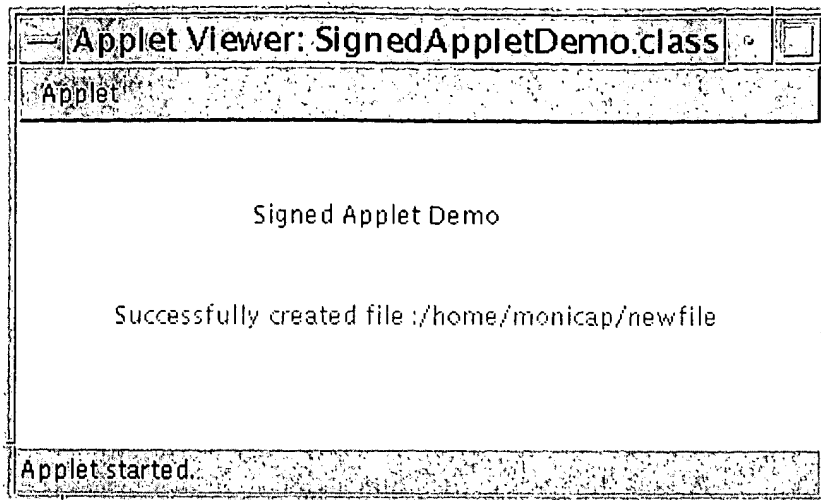
For a JDK 1.2 applet to access local system resources outside the directory from which the applet is launched, the applet must be granted explicit access to those resources. An applet is granted access to specific resources by setting up a policy file that contains the URLs to one or more resources that specifies the required permissions. When the applet is launched, it must be launched with the policy file to gain the access. Sometimes the permissions in the policy file require an applet be signed to gain access to some URLs and not signed for access to others.

Example

If the policy file requires the applet to be signed, `anApplet` can get access to the file only if it has the correct signature. If it has the wrong signature or no signature, it will not get access to the file. The policy file might require a signature for writing, but no signature for reading. If `anApplet` has the correct signature, it will be able to write, but if it does not, `anApplet` will only be allowed to read.

Example

If a signature is needed for the access, the applet has to be bundled into a Java ARchive (JAR) file before it can be signed. This example shows you how to sign and grant permission to an applet so it can create `newFile` in the user's home directory when it executes in Applet Viewer. See the Security in JDK 1.2 trail in *The Java Tutorial* for additional information.



These files are used for the example. You can copy them to or create them in your working directory.

- SignedAppletDemo.java file containing the applet code
- Write.jp policy file granting access to the user's home directory
- Applet tag embedded in the SignedApplet.html file:

```
<applet code="SignedAppletDemo.class"
  archive="SSignedApplet.jar"
  width=400 height=400>
  <param name=file value="/etc/inet/hosts">
</applet>
```

Usually an applet is bundled and signed by one person and handed off to another who verifies the signature and runs the applet. In this example, Susan performs Steps 1 through 5 and Ray performs Steps 6 through 8. But, to keep things simple, all steps occur in the same working directory.

1. Compile the applet
2. Create a JAR file
3. Generate Keys
4. Sign the JAR file
5. Export the Public Key Certificate
6. Import the Certificate as a Trusted Certificate
7. Create the policy file
8. Run the applet

Susan

Susan bundles the applet executable in a JAR file, signs the JAR file, and exports the public key certificate.

1. Compile the Applet

In her working directory, Susan uses the `javac` command to compile the `SignedAppletDemo.java` class. The output from the `javac` command is the `SignedAppletDemo.class`.

```
javac SignedAppletDemo.java
```

2. Make a JAR File

Susan then makes the compiled `SignedAppletDemo.class` file into a JAR file. The `-cvf` option to the `jar` command creates a new archive (c), using verbose mode (v), and specifies the archive file name (f). The archive file name is `SignedApplet.jar`.

```
jar cvf SignedApplet.jar SignedAppletDemo.class
```


3. Generate Keys

Susan creates a keystore database named `susanstore` that has an entry for a newly generated public and private key pair with the public key in a certificate.

A JAR file is signed with the private key of the creator of the JAR file and the signature is verified by the recipient of the JAR file with the public key in the pair. The certificate is a statement from the owner of the private key that the public key in the pair has a particular value so the person using the public key can be assured the public key is authentic. Public and private keys must already exist in the keystore database before `jarsigner` can be used to sign or verify the signature on a JAR file.

In her working directory, Susan creates a keystore database and generates the keys:

```
keytool -genkey -alias signFiles -keystore susanstore -keypass kpil35 -dname
"cn=jones" -storepass ab987c
```

This `keytool -genkey` command invocation generates a key pair that is identified by the alias `signFiles`. Subsequent `keytool` command invocations use this alias and the key password (`-keypass kpil35`) to access the private key in the generated pair.

The generated key pair is stored in a keystore database called `susanstore` (`-keystore susanstore`) in the current directory, and accessed with the `susanstore` password (`-storepass ab987c`).

The `-dname "cn=jones"` option specifies an X.500 Distinguished Name with a `commonName (cn)` value. X.500 Distinguished Names identify entities for X.509 certificates.

You can view all `keytool` options and parameters by typing:

```
keytool -help
```

4. Sign the JAR File

JAR Signer is a command line tool for signing and verifying the signature on JAR files. In her working directory, Susan uses `jarsigner` to make a signed copy of the `SignedApplet.jar` file.

```
jarsigner -keystore susanstore -storepass ab987c -keypass kpil35 -signedjar
SSignedApplet.jar SignedApplet.jar signFiles
```

The `-storepass ab987c` and `-keystore susanstore` options specify the keystore database and password where the private key for signing the JAR file is stored. The `-keypass kpil35` option is the password to the private key, `SSignedApplet.jar` is the name of the signed JAR file, and `signFiles` is the alias to the private key. `jarsigner` extracts the certificate from the keystore whose entry is `signFiles` and attaches it to the generated signature of the signed JAR file.

5. Export the Public Key Certificate

The public key certificate is sent with the JAR file to the whoever is going to use the applet. That person uses the certificate to authenticate the signature on the JAR file. To send a certificate, you have to first export it.

The `-storepass ab987c` and `-keystore susanstore` options specify the keystore database and password where the private key for signing the JAR file is stored. The `-keypass kpil35` option is the password to the private key, `SSignedApplet.jar` is the name of the signed JAR file, and `signFiles` is the alias to the private key. `jarsigner` extracts the certificate from the keystore whose entry is `signFiles` and attaches it to the generated signature of the signed JAR file.

5: Export the Public Key Certificate

The public key certificate is sent with the JAR file to the whoever is going to use the applet. That person uses the certificate to authenticate the signature on the JAR file. To send a certificate, you have to first export it.

In her working directory, Susan uses `keytool` to copy the certificate from `susanstore` to a file named `SusanJones.cer` as follows:

```
keytool -export -keystore susanstore -storepass ab987c -alias signFiles -file
SusanJones.cer
```

Ray

Ray receives the JAR file from Susan, imports the certificate, creates a policy file granting the applet access, and runs the applet.

6. Import Certificate as a Trusted Certificate

Ray has received `SSignedApplet.jar` and `SusanJones.cer` from Susan. He puts them in his home directory. Ray must now create a keystore database (`raystore`) and import the certificate into it. Ray uses `keytool` in his home directory `/home/ray` to import the certificate:

```
keytool -import -alias susan -file SusanJones.cer -keystore raystore -storepass abcdefg
```

7. Create the Policy File

The policy file grants the `SSignedApplet.jar` file signed by the alias `susan` permission to create `newfile` (and not other file) in the user's home directory.

Ray creates the policy file in his home directory using either `policytool` or an ASCII editor.

```
keystore "/home/ray/raystore";
// A sample policy file that lets a JavaTM program
// create newfile in user's home directory
// Satya N Dodda

grant SignedBy "susan" {
    permission java.util.PropertyPermission
        "user.home", "read"
    permission java.io.FilePermission
        "${user.home}/newfile", "write"
};
```

8. Run the Applet in Applet Viewer

Applet Viewer connects to the HTML documents and resources specified in the call to `appletviewer`, and displays the applet in its own window. To run the example, Ray copies the signed JAR file and HTML file to `/home/aURL/public_html` and invokes Applet viewer from his home directory as follows:

```
appletviewer -J-Djava.security.policy=Write.jp
http://aURL.com/SignedApplet.html
```

Note: Type everything on one line and put a space after `Write.jp`

The `-J-Djava.security.policy=Write.jp` option tells Applet Viewer to run the applet referenced in the `SignedApplet.html` file with the `Write.jp` policy file.

Note: The Policy file can be stored on a server and specified in the `appletviewer` invocation as a URL.

Signed Applets in JDK 1.1

JDK 1.1 signed applets can access local system resources if the local system is properly set up to allow it. See the JDK 1.1 Signed Applet Example page for details.

Conclusion

It is easy to use the JDK 1.2 security tools to sign a JAR file and allow an applet or application access to only certain specific resources. Just remember a JDK 1.2 applet will not run in a browser that is not enabled for JDK 1.2.

The JDC has a related article on security tools that explains the new JDK 1.2 security architecture and tools in more detail.

Visit the Security page on java.sun.com for documents that describe the JDK 1.2 security architecture, policy file, and keytool and jarsigner tools.

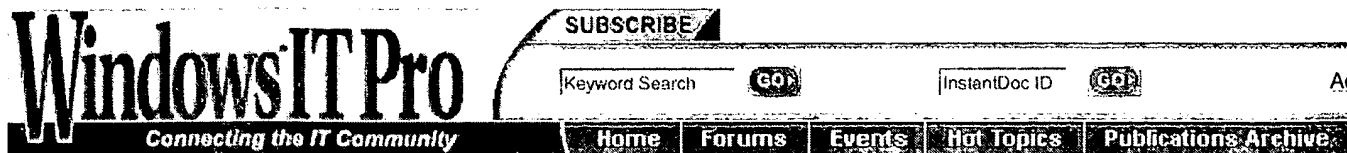


Monica Pawlan, a staff writer for the Java Developer Connection (JDC), is author of *Essentials of the Java Programming Language: A Hands-On Guide* (Addison-Wesley, 2000), and co-author of *Advanced Programming for the Java 2 Platform* (Addison-Wesley, 2000).

Satya Dodda is a JavaSoft engineer working in the security area.

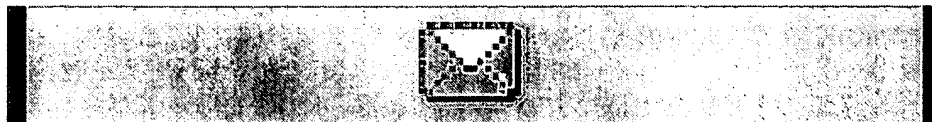
copyright © Sun Microsystems, Inc

APPENDIX II. H.



Related Hot Topics: Security

→→ Monthly Pass! [sign up now for \\$5.95/month!](#)



[Discoveries]

IE Unauthorized Cookie Access

Editors
InstantDoc #9433

IE Unauthorized Cookie Access

Reported May 19 by Marc Slemko

VERSIONS EFFECTED

- Internet Explorer 4.x
- Internet Explorer 5.x

DESCRIPTION

By design, the IE security model restricts cookies so that they can be read only by sites within the originator's domain. However, by using a specially-malformed URL, it is possible for a malicious web site operator to gain access to another site's cookie and read, add or change them. A malicious web site operator would need to entice a visiting user into clicking a link in order to access each cookie, and could not obtain a listing of the cookies available on the visitor's system. Even after recovering a cookie, the type and amount of personal information would depend on the privacy practices followed by the site that placed it there.

VENDOR RESPONSE

Microsoft has issued a [patch](#) for the problem.

The patches require IE 4.01 Service Pack 2 or IE 5.01 to install. Customers using versions prior to these may receive a message reading "This update does not need to be installed on this system". This message is incorrect. More information is available in KB article [Q262509](#).

- Frequently Asked Questions: Microsoft Security Bulletin MS00-033,
<http://www.microsoft.com/technet/security/bulletin/fq00-033.asp>

APPENDIX II. I.

Web Site May Retrieve Cookies from Your Computer

This article was previously published under Q258430

Article ID : 258430

Last Review : November 26, 2003

Revision : 3.0

SYMPTOMS

When you use Internet Explorer to visit a Web site, the Web site may be able to retrieve cookies that were not created by that Web site from your computer.

RESOLUTION

To resolve this problem, obtain the latest service pack for Internet Explorer version 5.01. For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

[267954](#) How to Obtain the Latest Internet Explorer 5.01 Service Pack

For additional information about resolving this problem, click the article number below to view the article in the Microsoft Knowledge Base:

[262509](#) Patch Available for "Frame Domain Verification," "Unauthorized Cookie Access," "Malformed Component Attribute," and "WPAD Spoofing" Vulnerabilities

STATUS

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article. This problem was first corrected in Internet Explorer version 5.01 Service Pack 1. This issue also occurs with Internet Explorer version 5.5 Beta, but there is no update available for this Beta release. This issue is resolved in the final release of Internet Explorer 5.5.

APPLIES TO

- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.0
- Microsoft Internet Explorer 4.01 Service Pack 1
- Microsoft Internet Explorer 4.01 Service Pack 2
- Microsoft Internet Explorer 4.0 128-Bit Edition
- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.0
- Microsoft Internet Explorer 4.01 Service Pack 2
- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.0
- Microsoft Internet Explorer 4.01 Service Pack 1
- Microsoft Internet Explorer 4.01 Service Pack 2
- Microsoft Internet Explorer 4.0 128-Bit Edition
- the operating system: Microsoft Windows 2000

Keywords: kbbug kbfix kbie501presp1fix KB258430

APPENDIX II. J.



PERSISTENT CLIENT STATE HTTP COOKIES

Preliminary Specification - Use with caution

INTRODUCTION

Cookies are a general mechanism which server side connections (such as CGI scripts) can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of Web-based client/server applications.

OVERVIEW

A server, when returning an HTTP object to a client, may also send a piece of state information which the client will store. Included in that state object is a description of the range of URLs for which that state is valid. Any future HTTP requests made by the client which fall in that range will include a transmittal of the current value of the state object from the client back to the server. The state object is called a **cookie**, for no compelling reason.

This simple mechanism provides a powerful new tool which enables a host of new types of applications to be written for web-based environments. Shopping applications can now store information about the currently selected items, for fee services can send back registration information and free the client from retyping a user-id on next connection, sites can store per-user preferences on the client, and have the client supply those preferences every time that site is connected to.

SPECIFICATION

A cookie is introduced to the client by including a **Set-Cookie** header as part of an HTTP response, typically this will be generated by a CGI script.

Syntax of the Set-Cookie HTTP Response Header

This is the format a CGI script would use to add to the HTTP headers a new piece of data which is to be stored by the client for later retrieval.

```
Set-Cookie: NAME=VALUE; expires=DATE;  
path=PATH; domain=DOMAIN_NAME; secure
```

NAME=VALUE

This string is a sequence of characters excluding semi-colon, comma and white space. If there is a

need to place such data in the name or value, some encoding method such as URL style %XX encoding is recommended, though no encoding is defined or required.

This is the only required attribute on the **Set-Cookie** header.

expires=DATE

The **expires** attribute specifies a date string that defines the valid life time of that cookie. Once the expiration date has been reached, the cookie will no longer be stored or given out.

The date string is formatted as:

Wdy, DD-Mon-YYYY HH:MM:SS GMT

This is based on [RFC 822](#), [RFC 850](#), [RFC 1036](#), and [RFC 1123](#), with the variations that the only legal time zone is **GMT** and the separators between the elements of the date must be dashes.

expires is an optional attribute. If not specified, the cookie will expire when the user's session ends.

Note: There is a bug in Netscape Navigator version 1.1 and earlier. Only cookies whose **path** attribute is set explicitly to "/" will be properly saved between sessions if they have an **expires** attribute.

domain=DOMAIN_NAME

When searching the cookie list for valid cookies, a comparison of the **domain** attributes of the cookie is made with the Internet domain name of the host from which the URL will be fetched. If there is a tail match, then the cookie will go through **path** matching to see if it should be sent. "Tail matching" means that **domain** attribute is matched against the tail of the fully qualified domain name of the host. A **domain** attribute of "acme.com" would match host names "anvil.acme.com" as well as "shipping.crate.acme.com".

Only hosts within the specified domain can set a cookie for a domain and domains must have at least two (2) or three (3) periods in them to prevent domains of the form: ".com", ".edu", and ".va.us". Any domain that fails within one of the seven special top level domains listed below only require two periods. Any other domain requires at least three. The seven special top level domains are: "COM", "EDU", "NET", "ORG", "GOV", "MIL", and "INT".

The default value of **domain** is the host name of the server which generated the cookie response.

path=PATH

The **path** attribute is used to specify the subset of URLs in a domain for which the cookie is valid. If a cookie has already passed **domain** matching, then the pathname component of the URL is compared with the path attribute, and if there is a match, the cookie is considered valid and is sent along with the URL request. The path "/foo" would match "/foobar" and "/foo/bar.html". The path "/" is the most general path.

If the **path** is not specified, it is assumed to be the same path as the document being described by the header which contains the cookie.

secure

If a cookie is marked **secure**, it will only be transmitted if the communications channel with the host is a secure one. Currently this means that secure cookies will only be sent to HTTPS (HTTP over SSL) servers.

If **secure** is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

Syntax of the Cookie HTTP Request Header

When requesting a URL from an HTTP server, the browser will match the URL against all cookies and if any of them match, a line containing the name/value pairs of all matching cookies will be included in the HTTP request. Here is the format of that line:

Cookie: *NAME1=OPAQUE_STRING1; NAME2=OPAQUE_STRING2 ...*

Additional Notes

- Multiple **Set-Cookie** headers can be issued in a single server response.
- Instances of the same path and name will overwrite each other, with the latest instance taking precedence. Instances of the same path but different names will add additional mappings.
- Setting the path to a higher-level value does not override other more specific path mappings. If there are multiple matches for a given cookie name, but with separate paths, all the matching cookies will be sent. (See examples below.)
- The expires header lets the client know when it is safe to purge the mapping but the client is not required to do so. A client may also delete a cookie before it's expiration date arrives if the number of cookies exceeds its internal limits.
- When sending cookies to a server, all cookies with a more specific path mapping should be sent before cookies with less specific path mappings. For example, a cookie "name1=foo" with a path mapping of "/" should be sent after a cookie "name1=foo2" with a path mapping of "/bar" if they are both to be sent.
- There are limitations on the number of cookies that a client can store at any one time. This is a specification of the minimum number of cookies that a client should be prepared to receive and store.
 - 300 total cookies
 - 4 kilobytes per cookie, where the name and the OPAQUE_STRING combine to form the 4 kilobyte limit.
 - 20 cookies per server or domain. (note that completely specified hosts and domains are treated as separate entities and have a 20 cookie limitation for each, not combined)Servers should not expect clients to be able to exceed these limits. When the 300 cookie limit or the 20 cookie per server limit is exceeded, clients should delete the least recently used cookie. When a cookie larger than 4 kilobytes is encountered the cookie should be trimmed to fit, but the name should remain intact as long as it is less than 4 kilobytes.
- If a CGI script wishes to delete a cookie, it can do so by returning a cookie with the same name, and an **expires** time which is in the past. The path and name must match exactly in order for the

expiring cookie to replace the valid cookie. This requirement makes it difficult for anyone but the originator of a cookie to delete a cookie.

- When caching HTTP, as a proxy server might do, the **Set-cookie** response header should never be cached.
- If a proxy server receives a response which contains a **Set-cookie** header, it should propagate the **Set-cookie** header to the client, regardless of whether the response was 304 (Not Modified) or 200 (OK).

Similarly, if a client request contains a Cookie: header, it should be forwarded through a proxy, even if the conditional If-modified-since request is being made.

EXAMPLES

Here are some sample exchanges which are designed to illustrate the use of cookies.

First Example transaction sequence:

Client requests a document, and receives in the response:

```
Set-Cookie: CUSTOMER=WILE_E_COYOTE; path=/; expires=Wednesday, 09-Nov-99 23:12:
```

When client requests a URL in path "/" on this server, it sends:

```
Cookie: CUSTOMER=WILE_E_COYOTE
```

Client requests a document, and receives in the response:

```
Set-Cookie: PART_NUMBER=ROCKET_LAUNCHER_0001; path=
```

When client requests a URL in path "/" on this server, it sends:

```
Cookie: CUSTOMER=WILE_E_COYOTE; PART_NUMBER=ROCKET_LAUNCHER_0001
```

Client receives:

```
Set-Cookie: SHIPPING=FEDEX; path=/foo
```

When client requests a URL in path "/" on this server, it sends:

```
Cookie: CUSTOMER=WILE_E_COYOTE; PART_NUMBER=ROCKET_LAUNCHER_0001
```

When client requests a URL in path "/foo" on this server, it sends:

```
Cookie: CUSTOMER=WILE_E_COYOTE; PART_NUMBER=ROCKET_LAUNCHER_0001; SHIPPING=FEDE
```

Second Example transaction sequence:

Assume all mappings from above have been cleared.

Client receives:

Set-Cookie: PART_NUMBER=ROCKET_LAUNCHER_0001; path=/
When client requests a URL in path "/" on this server, it sends:

Cookie: PART_NUMBER=ROCKET_LAUNCHER_0001

Client receives:

Set-Cookie: PART_NUMBER=RIDING_ROCKET_0023; path=/ammo

When client requests a URL in path "/ammo" on this server, it sends:

Cookie: PART_NUMBER=RIDING_ROCKET_0023; PART_NUMBER=ROCKET_LAUNCHER_0001

NOTE: There are two name/value pairs named "PART_NUMBER" due to the inheritance of the "/" mapping in addition to the "/ammo" mapping.

[Help](#) | [Site Map](#) | [How to Get Netscape Products](#) | [Advertise With Us](#) | [Add Site](#) | [Custom Browser Program](#)

[Autos](#) | [Business](#) | [Computing & Internet](#) | [Entertainment](#) | [Family](#) | [Games](#) | [Health](#) | [Lifestyles](#) | [Local](#) | [Netscape](#) | [Netscape Open Directory](#) | [News](#) | [Personal Finance](#) | [Real Estate](#) | [Research & Learn](#) | [Shopping](#) | [Small Business](#) | [Sports](#) | [Travel](#)

© 1999 Netscape, All Rights Reserved. [Legal & Privacy Notices](#)
This site powered by [Netscape SuiteSpot servers](#).

APPENDIX II. K.

HTTP Working Group
INTERNET DRAFT
<draft-kristol-http-state-info-00.txt>
August 25, 1995

David M. Kristol
AT&T Bell Laboratories
Expires February 25, 1995

Proposed HTTP State-Info Mechanism

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``lid-abstracts.txt' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

This is author's draft 1.12.

1. ABSTRACT

HTTP, the protocol that underpins the World-Wide Web (WWW), is stateless. That is, each request stands on its own; origin servers don't need to remember what happened with previous requests to service a new one. Statelessness is a mixed blessing, because there are potential WWW applications, like ``shopping baskets' and library browsing, for which the history of a user's actions is useful or essential.

This proposal outlines a way to introduce state into HTTP. A new request/response header, State-Info, carries the state back and forth, thus relieving the origin server from needing to keep an extensive per-user or per-connection database. The changes required to user agents, origin servers, and proxy servers to support State-Info are very modest.

2. TERMINOLOGY

The terms user agent, client, server, proxy, and origin server have the same meaning as in the HTTP/1.0 specification.

INTERNET DRAFT Proposed HTTP State-Info Mechanism August 25, 1995

3. STATE AND SESSIONS

This proposal outlines how to introduce state into HTTP, the protocol that underpins the World-Wide Web (WWW). At present, HTTP is stateless: a WWW origin server obtains everything it needs to know about a request from the request itself. After it processes the request, the origin server can ``forget'' the transaction.

What do I mean by ``state?'' ``State'' implies some relation between one request to an origin server and previous ones made by the same user agent to the same origin server. If the sequence of these requests is considered as a whole, they can be thought of as a ``session.''

Koen Holtman identified these dimensions for the ``solution space'' of stateful dialogs:

- +□o simplicity of implementation
- +□o simplicity of use
- +□o time of general availability when standardized
- +□o downward compatibility
- +□o reliability
- +□o amount of privacy protection
- +□o maximum complexity of stateful dialogs supported
- +□o amount of cache control possible
- +□o risks when used with non-conforming caches

The paradigm I have in mind obtains the same effect as if a user agent connected to an origin server, carried out many transactions at the user's direction, then disconnected. Two example applications I have in mind are a ``shopping cart,'' where the state information comprises what the user has bought, and a magazine browsing system, where the state information comprises the set of journals and articles the user has looked at already. Note some of the key points in the session paradigm:

1. The session has a beginning and an end.
2. The session is relatively short-lived.
3. Either the user agent or the origin server may terminate a session.

4. State is a property of the connection to the origin server. The user agent itself has no special state information. (However,

Kristol

draft-kristol-http-state-info-00.txt

[Page 2]

INTERNET DRAFT

Proposed HTTP State-Info Mechanism

August 25, 1995

what the user agent presents to the user may reflect the origin server's state, because the origin server returns that information to the user agent.)

4. PROPOSAL OUTLINE

The proposal I outline here defines a way for an origin server to send state information to the user agent, and for the user agent to return the state information to the origin server. The goal of the proposal is to have a minimal impact on HTTP and user agents. Only origin servers that need to maintain sessions would suffer any significant impact.

4.1 Origin Server Role

The origin server initiates a session, if it so desires. (Note that ``session'' here is a logical connection, not a physical one. Don't confuse these logical sessions with various ``keepalive'' proposals for physical sessions.) To initiate a session, the origin server returns an extra response header to the client:

State-Info: opaque information

The opaque information may be anything the origin server chooses to send, encoded in printable ASCII. ``Opaque'' implies that the content is of interest and relevance only to the origin server. The content may, in fact, be readable by anyone that examines the State-Info header.

If the origin server gets a State-Info request header from the client (see below), it may ignore it or use it to determine the current state of the session. It may send back to the client the same, a different, or no State-Info response header. The origin server effectively ends a session by sending back a State-Info header with no value.

4.2 User Agent Role

The user agent keeps track of State-Info for each origin server (distinguished by name or IP address and port). The extent of its bookkeeping is to note that it does or does not have State-Info for the origin server.

The user agent goes from the ``no State-Info'' state to the ``have State-Info'' state when it receives a non-empty State-Info response

header from the origin server. (The user agent saves the State-Info value.) It returns to the ``no State-Info'' state if it receives a State-Info response header with no value. It stays in the ``have State-Info'' state if it receives a non-empty State-Info response header; the new value overwrites the old one. If the user agent receives no State-Info response header, it stays in the same state (``have State-Info'' or ``no State-Info''). The behavior described above applies for all response codes from the origin server.

Kristol

draft-kristol-http-state-info-00.txt

[Page 3]

INTERNET DRAFT

Proposed HTTP State-Info Mechanism

August 25, 1995

When it sends a request to an origin server, the user agent sends a State-Info request header if it's in the ``have State-Info'' state; otherwise it sends no State-Info request header.

A user agent usually begins execution with no remembered State-Info information. The user agent may be configured never to send State-Info, in which case it can never sustain state with an origin server. (This would also be true of user agents that are unaware of how to handle State-Info.)

A user agent (at the user's direction) can terminate a session with an origin server by discarding the associated State-Info information (moving to the ``no State-Info'' state).

When the user agent terminates execution, it discards all State-Info information. Alternatively, the user agent may ask the user whether State-Info should be retained; the default should be ``no.''. Retained State-Info would then be restored when the user agent begins execution again.

User agent programs that can display multiple independent windows should behave as if each window were a separate program instance with respect to State-Info. Thus State-Info obtained in one window would have no effect on links followed in another. (The user agent would have to store State-Info tagged by window number, as well as origin server address and port.) When a window terminates, all associated State-Info information gets discarded.

4.3 Caching Proxy Role

One reason for separating state information from both a URL and document content is to facilitate the scaling that caching permits. A caching proxy

- +□o must pass along a State-Info request header from the requesting client to the next server, even if it has cached the requested resource locally. (I originally assumed that requests from a cache

always resulted in a conditional GET request to the next server, and that a State-Info header could ride along for free. Such is not the case, and passing along State-Info headers, which is an essential part of this proposal, could be expensive.)

+□o must pass back to the client any State-Info response header it receives.

+□o may cache the received response, but must not cache the State-Info header as part of its cache state. (Caching the response is subject to the control of the usual headers, such as Expires and Pragma: no-cache.)

Kristol

draft-kristol-http-state-info-00.txt

[Page 4]

INTERNET DRAFT

Proposed HTTP State-Info Mechanism

August 25, 1995

5. IMPLEMENTATION CONSIDERATIONS

Here I speculate on likely or desirable details for an origin server that implements Server-Info.

5.1 State-Info Content

An origin server's content should probably be divided into disjoint application areas, some of which require the use of State-Info. The application areas can be distinguished by their request URLs. The State-Info header can incorporate information about multiple sessions that a user agent might start as follows. Imagine that a single session's state information takes the form

URL opaque

The opaque information might be a uuencoding of application-specific information. The URL might be the actual URL of a resource, or it might be the prefix for all URLs that comprise a particular application. The State-Info header for multiple sessions can be formed by concatenating the session state information of all sessions, separated by commas, as in

State-Info: /A YXBwbGljYXRpb246MQ==, /B YXBwbGljYXRpb246Mg==

The session information can obviously be clear or encoded text that describes state. However, if it grows too large, it can become unwieldy. Therefore, an implementor might choose for the session information to be a key into a server-side database. Of course, using a database creates some problems that the State-Info proposal was meant to avoid, namely:

1. keeping real state on the server side;
2. how and when to garbage-collect the database entry, in case the user agent terminates the session by, for example, exiting.

The origin server software should probably be designed to separate the session information for different applications and only present to a particular application the session information that applies to it.

5.2 Stateless Pages

Caching is a good thing for the scalability of WWW. Therefore it's important to reduce the number of documents that have state embedded in them inherently. For example, if a shopping-basket-style application always displayed a user's current basket contents on each page, those pages could not be cached, because each user's basket's contents would be different. On the other hand, if each page contained just a link that allowed the user to ``Look at My Shopping Basket,`` the page could be cached.

Kristol draft-kristol-http-state-info-00.txt [Page 5]

INTERNET DRAFT Proposed HTTP State-Info Mechanism August 25, 1995

6. PRIVACY

An origin server can create a State-Info header to track the path of a user through the server. Users may object to this behavior as intrusive accumulation of information, although their identity is not evident. (Identity might become evident if a user fills out a form that contains identifying information.) The State-Info proposal therefore gives a user some control over this possible intrusion by

- +□o Recommending that a user agent should be able, as a configuration option, never to create stateful sessions.
- +□o Recommending that a user agent allow a user to discard State-Info at any time.
- +□o Recommending that terminating a user agent's execution (or the execution of a window, for multi-window user agents) causes State-Info to be discarded.

7. OTHER, SIMILAR, PROPOSALS

I'm aware of two other proposals to accomplish similar goals. Netscape proposes a Cookie request header and Set-Cookie response header. Netscape cookies have expiration times and other information that

require more complicated processing by the user agent than does my proposal. Furthermore, there's no requirement that cookies be discarded when the user exits a user agent program.

Brian Behlendorf proposed a Session-ID header that would be user-agent-initiated and could be used by an origin server to track ``clickstreams.'' It would not carry any origin-server-defined state, however.

Koen Holtman has made a proposal that is similar in flavor to, but different in detail from, this one.

8. SECURITY CONSIDERATIONS

The information in the State-Info headers is unprotected. Two consequences are:

1. Any sensitive information that is conveyed in a State-Info header is exposed to intruders.
2. A malicious intermediary could alter the State-Info header as it travels in either direction, with unpredictable results.

These facts imply that information of a personal and/or financial nature should only be sent over a secure channel. For less sensitive

Kristol draft-kristol-http-state-info-00.txt [Page 6]

INTERNET DRAFT Proposed HTTP State-Info Mechanism August 25, 1995

information, or when the content of the header is a database key, an origin server should be vigilant to prevent a bad Session-Info value from causing it to fail.

9. ACKNOWLEDGEMENTS

My thanks go to correspondents on the http-wg and www-talk mailing lists who contributed ideas and criticism that found its way into this proposal. Special thanks to Bob Wyman, Koen Holtman, Shel Kaphan.

10. AUTHOR'S ADDRESS

David M. Kristol
AT&T Bell Laboratories
600 Mountain Ave. Room 2A-227
Murray Hill, NJ 07974

Phone: (908) 582-2250
FAX: (908) 582-5809
Email: dmkk@research.att.com

Kristol

draft-kristol-http-state-info-00.txt

[Page 7]

APPENDIX II. L.



RFC 2109 (RFC2109)

Internet RFC/STD/FYI/BCP Archives

[[RFC Index](#) | [RFC Search](#) | [Usenet FAQs](#) | [Web FAQs](#) | [Documents](#) | [Cities](#)]

Alternate Formats: [rfc2109.txt](#) | [rfc2109.txt.pdf](#)

[Comment on RFC 2109](#)

RFC 2109 - HTTP State Management Mechanism

Network Working Group
Request for Comments: 2109
Category: Standards Track

D. Kristol
Bell Laboratories, Lucent Technologies
L. Montulli
Netscape Communications
February 1997

HTTP State Management Mechanism

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

1. ABSTRACT

This document specifies a way to create a stateful session with HTTP requests and responses. It describes two new headers, Cookie and Set-Cookie, which carry state information between participating origin servers and user agents. The method described here differs from Netscape's Cookie proposal, but it can interoperate with HTTP/1.0 user agents that use Netscape's method. (See the HISTORICAL section.)

2. TERMINOLOGY

The terms user agent, client, server, proxy, and origin server have the same meaning as in the HTTP/1.0 specification.

Fully-qualified host name (FQHN) means either the fully-qualified domain name (FQDN) of a host (i.e., a completely specified domain name ending in a top-level domain such as .com or .uk), or the numeric Internet Protocol (IP) address of a host. The fully qualified domain name is preferred; use of numeric IP addresses is

strongly discouraged.

The terms request-host and request-URI refer to the values the client would send to the server as, respectively, the host (but not port) and abs_path portions of the absoluteURI (http_URL) of the HTTP request line. Note that request-host must be a FQHN.

Hosts names can be specified either as an IP address or a FQHN string. Sometimes we compare one host name with another. Host A's name domain-matches host B's if

- * both host names are IP addresses and their host name strings match exactly; or
- * both host names are FQDN strings and their host name strings match exactly; or
- * A is a FQDN string and has the form NB, where N is a non-empty name string, B has the form .B', and B' is a FQDN string. (So, x.y.com domain-matches .y.com but not y.com.)

Note that domain-match is not a commutative operation: a.b.c.com domain-matches .c.com, but not the reverse.

Because it was used in Netscape's original implementation of state management, we will use the term cookie to refer to the state information that passes between an origin server and user agent, and that gets stored by the user agent.

3. STATE AND SESSIONS

This document describes a way to create stateful sessions with HTTP requests and responses. Currently, HTTP servers respond to each client request without relating that request to previous or subsequent requests; the technique allows clients and servers that wish to exchange state information to place HTTP requests and responses within a larger context, which we term a "session". This context might be used to create, for example, a "shopping cart", in which user selections can be aggregated before purchase, or a magazine browsing system, in which a user's previous reading affects which offerings are presented.

There are, of course, many different potential contexts and thus many different potential types of session. The designers' paradigm for sessions created by the exchange of cookies has these key attributes:

1. Each session has a beginning and an end.
2. Each session is relatively short-lived.
3. Either the user agent or the origin server may terminate a session.
4. The session is implicit in the exchange of state information.

4. OUTLINE

We outline here a way for an origin server to send state information to the user agent, and for the user agent to return the state information to the origin server. The goal is to have a minimal

impact on HTTP and user agents. Only origin servers that need to maintain sessions would suffer any significant impact, and that impact can largely be confined to Common Gateway Interface (CGI) programs, unless the server provides more sophisticated state management support. (See Implementation Considerations, below.)

4.1 Syntax: General

The two state management headers, Set-Cookie and Cookie, have common syntactic properties involving attribute-value pairs. The following grammar uses the notation, and tokens DIGIT (decimal digits) and token (informally, a sequence of non-special, non-white space characters) from the HTTP/1.1 specification [RFC 2068] to describe their syntax.

```
av-pairs      =      av-pair *(";" av-pair)
av-pair       =      attr ["=" value]          ; optional value
attr          =      token
value         =      word
word          =      token | quoted-string
```

Attributes (names) (attr) are case-insensitive. White space is permitted between tokens. Note that while the above syntax description shows value as optional, most attrs require them.

NOTE: The syntax above allows whitespace between the attribute and the = sign.

4.2 Origin Server Role

4.2.1 General

The origin server initiates a session, if it so desires. (Note that "session" here does not refer to a persistent network connection but to a logical session created from HTTP requests and responses. The presence or absence of a persistent connection should have no effect on the use of cookie-derived sessions). To initiate a session, the origin server returns an extra response header to the client, Set-Cookie. (The details follow later.)

A user agent returns a Cookie request header (see below) to the origin server if it chooses to continue a session. The origin server may ignore it or use it to determine the current state of the

session. It may send back to the client a Set-Cookie response header with the same or different information, or it may send no Set-Cookie header at all. The origin server effectively ends a session by sending the client a Set-Cookie header with Max-Age=0.

Servers may return a Set-Cookie response headers with any response. User agents should send Cookie request headers, subject to other rules detailed below, with every request.

An origin server may include multiple Set-Cookie headers in a response. Note that an intervening gateway could fold multiple such headers into a single header.

4.2.2 Set-Cookie Syntax

The syntax for the Set-Cookie response header is

```

set-cookie      =      "Set-Cookie:" cookies
cookies         =      1#cookie
cookie          =      NAME "=" VALUE *("; " cookie-av)
NAME            =      attr
VALUE           =      value
cookie-av       =      "Comment" "=" value
                  |      "Domain" "=" value
                  |      "Max-Age" "=" value
                  |      "Path" "=" value
                  |      "Secure"
                  |      "Version" "=" 1*DIGIT

```

Informally, the Set-Cookie response header comprises the token Set-Cookie:, followed by a comma-separated list of one or more cookies. Each cookie begins with a NAME=VALUE pair, followed by zero or more semi-colon-separated attribute-value pairs. The syntax for attribute-value pairs was shown earlier. The specific attributes and the semantics of their values follows. The NAME=VALUE attribute-value pair must come first in each cookie. The others, if present, can occur in any order. If an attribute appears more than once in a cookie, the behavior is undefined.

NAME=VALUE

Required. The name of the state information ("cookie") is NAME, and its value is VALUE. NAMES that begin with \$ are reserved for other uses and must not be used by applications.

The VALUE is opaque to the user agent and may be anything the origin server chooses to send, possibly in a server-selected printable ASCII encoding. "Opaque" implies that the content is of interest and relevance only to the origin server. The content may, in fact, be readable by anyone that examines the Set-Cookie header.

Comment=comment

Optional. Because cookies can contain private information about a user, the Cookie attribute allows an origin server to document its intended use of a cookie. The user can inspect the information to decide whether to initiate or continue a session with this cookie.

Domain=domain

Optional. The Domain attribute specifies the domain for which the cookie is valid. An explicitly specified domain must always start with a dot.

Max-Age=delta-seconds

Optional. The Max-Age attribute defines the lifetime of the cookie, in seconds. The delta-seconds value is a decimal non-negative integer. After delta-seconds seconds elapse, the client should discard the cookie. A value of zero means the cookie should be discarded immediately.

Path=path

Optional. The Path attribute specifies the subset of URLs to which this cookie applies.

Secure

Optional. The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin

server whenever it sends back this cookie.

The user agent (possibly under the user's control) may determine what level of security it considers appropriate for "secure" cookies. The Secure attribute should be considered security advice from the server to the user agent, indicating that it is in the session's interest to protect the cookie contents.

Version=version

Required. The Version attribute, a decimal integer, identifies to which version of the state management specification the cookie conforms. For this specification, Version=1 applies.

4.2.3 Controlling Caching

An origin server must be cognizant of the effect of possible caching of both the returned resource and the Set-Cookie header. Caching "public" documents is desirable. For example, if the origin server wants to use a public document such as a "front door" page as a sentinel to indicate the beginning of a session for which a Set-Cookie response header must be generated, the page should be stored in caches "pre-expired" so that the origin server will see further requests. "Private documents", for example those that contain information strictly private to a session, should not be cached in shared caches.

If the cookie is intended for use by a single user, the Set-cookie header should not be cached. A Set-cookie header that is intended to be shared by multiple users may be cached.

The origin server should send the following additional HTTP/1.1 response headers, depending on circumstances:

- * To suppress caching of the Set-Cookie header: Cache-control: no-cache="set-cookie".

and one of the following:

- * To suppress caching of a private document in shared caches: Cache-control: private.
- * To allow caching of a document and require that it be validated before returning it to the client: Cache-control: must-revalidate.
- * To allow caching of a document, but to require that proxy caches (not user agent caches) validate it before returning it to the client: Cache-control: proxy-revalidate.
- * To allow caching of a document and request that it be validated before returning it to the client (by "pre-expiring" it): Cache-control: max-age=0. Not all caches will revalidate the document in every case.

HTTP/1.1 servers must send Expires: old-date (where old-date is a date long in the past) on responses containing Set-Cookie response headers unless they know for certain (by out of band means) that there are no downstream HTTP/1.0 proxies. HTTP/1.1 servers may send other Cache-Control directives that permit caching by HTTP/1.1 proxies in addition to the Expires: old-date directive; the Cache-Control directive will override the Expires: old-date for HTTP/1.1

proxies.

4.3 User Agent Role

4.3.1 Interpreting Set-Cookie

The user agent keeps separate track of state information that arrives via Set-Cookie response headers from each origin server (as distinguished by name or IP address and port). The user agent applies these defaults for optional attributes that are missing:

Version Defaults to "old cookie" behavior as originally specified by Netscape. See the HISTORICAL section.

Domain Defaults to the request-host. (Note that there is no dot at the beginning of request-host.)

Max-Age The default behavior is to discard the cookie when the user agent exits.

Path Defaults to the path of the request URL that generated the Set-Cookie response, up to, but not including, the right-most /.

Secure If absent, the user agent may send the cookie over an insecure channel.

4.3.2 Rejecting Cookies

To prevent possible security or privacy violations, a user agent rejects a cookie (shall not store its information) if any of the following is true:

- * The value for the Path attribute is not a prefix of the request-URI.
- * The value for the Domain attribute contains no embedded dots or does not start with a dot.
- * The value for the request-host does not domain-match the Domain attribute.
- * The request-host is a FQDN (not IP address) and has the form HD, where D is the value of the Domain attribute, and H is a string that contains one or more dots.

Examples:

- * A Set-Cookie from request-host y.x.foo.com for Domain=.foo.com would be rejected, because H is y.x and contains a dot.
- * A Set-Cookie from request-host x.foo.com for Domain=.foo.com would be accepted.
- * A Set-Cookie with Domain=.com or Domain=.com., will always be rejected, because there is no embedded dot.
- * A Set-Cookie with Domain=ajax.com will be rejected because the value for Domain does not begin with a dot.

4.3.3 Cookie Management

If a user agent receives a Set-Cookie response header whose NAME is the same as a pre-existing cookie, and whose Domain and Path attribute values exactly (string) match those of a pre-existing cookie, the new cookie supersedes the old. However, if the Set-Cookie has a value for Max-Age of zero, the (old and new) cookie is discarded. Otherwise cookies accumulate until they expire (resources permitting), at which time they are discarded.

Because user agents have finite space in which to store cookies, they may also discard older cookies to make space for newer ones, using, for example, a least-recently-used algorithm, along with constraints on the maximum number of cookies that each origin server may set.

If a Set-Cookie response header includes a Comment attribute, the user agent should store that information in a human-readable form with the cookie and should display the comment text as part of a cookie inspection user interface.

User agents should allow the user to control cookie destruction. An infrequently-used cookie may function as a "preferences file" for network applications, and a user may wish to keep it even if it is the least-recently-used cookie. One possible implementation would be an interface that allows the permanent storage of a cookie through a checkbox (or, conversely, its immediate destruction).

Privacy considerations dictate that the user have considerable control over cookie management. The PRIVACY section contains more information.

4.3.4 Sending Cookies to the Origin Server

When it sends a request to an origin server, the user agent sends a Cookie request header to the origin server if it has cookies that are applicable to the request, based on

- * the request-host;
- * the request-URI;
- * the cookie's age.

The syntax for the header is:

```

cookie           =      "Cookie:" cookie-version
                        1*("(" cookie-value
cookie-value     =      NAME "=" VALUE [";" path] [";" domain]
cookie-version   =      "$Version" "=" value
NAME             =      attr
VALUE            =      value
path             =      "$Path" "=" value
domain          =      "$Domain" "=" value

```

The value of the cookie-version attribute must be the value from the Version attribute, if any, of the corresponding Set-Cookie response header. Otherwise the value for cookie-version is 0. The value for the path attribute must be the value from the Path attribute, if any, of the corresponding Set-Cookie response header. Otherwise the attribute should be omitted from the Cookie request header. The

value for the domain attribute must be the value from the Domain attribute, if any, of the corresponding Set-Cookie response header. Otherwise the attribute should be omitted from the Cookie request header.

Note that there is no Comment attribute in the Cookie request header corresponding to the one in the Set-Cookie response header. The user agent does not return the comment information to the origin server.

The following rules apply to choosing applicable cookie-values from among all the cookies the user agent has.

Domain Selection

The origin server's fully-qualified host name must domain-match the Domain attribute of the cookie.

Path Selection

The Path attribute of the cookie must match a prefix of the request-URI.

Max-Age Selection

Cookies that have expired should have been discarded and thus are not forwarded to an origin server.

If multiple cookies satisfy the criteria above, they are ordered in the Cookie header such that those with more specific Path attributes precede those with less specific. Ordering with respect to other attributes (e.g., Domain) is unspecified.

Note: For backward compatibility, the separator in the Cookie header is semi-colon (;) everywhere. A server should also accept comma (,) as the separator between cookie-values for future compatibility.

4.3.5 Sending Cookies in Unverifiable Transactions

Users must have control over sessions in order to ensure privacy. (See PRIVACY section below.) To simplify implementation and to prevent an additional layer of complexity where adequate safeguards exist, however, this document distinguishes between transactions that are verifiable and those that are unverifiable. A transaction is verifiable if the user has the option to review the request-URI prior to its use in the transaction. A transaction is unverifiable if the user does not have that option. Unverifiable transactions typically arise when a user agent automatically requests inlined or embedded entities or when it resolves redirection (3xx) responses from an origin server. Typically the origin transaction, the transaction that the user initiates, is verifiable, and that transaction may directly or indirectly induce the user agent to make unverifiable transactions.

When it makes an unverifiable transaction, a user agent must enable a session only if a cookie with a domain attribute D was sent or received in its origin transaction, such that the host name in the Request-URI of the unverifiable transaction domain-matches D.

This restriction prevents a malicious service author from using unverifiable transactions to induce a user agent to start or continue a session with a server in a different domain. The starting or continuation of such sessions could be contrary to the privacy expectations of the user, and could also be a security problem.

User agents may offer configurable options that allow the user agent, or any autonomous programs that the user agent executes, to ignore the above rule, so long as these override options default to "off".

Many current user agents already provide a review option that would render many links verifiable. For instance, some user agents display the URL that would be referenced for a particular link when the mouse pointer is placed over that link. The user can therefore determine whether to visit that site before causing the browser to do so.

(Though not implemented on current user agents, a similar technique could be used for a button used to submit a form -- the user agent

could display the action to be taken if the user were to select that button.) However, even this would not make all links verifiable; for example, links to automatically loaded images would not normally be subject to "mouse pointer" verification.

Many user agents also provide the option for a user to view the HTML source of a document, or to save the source to an external file where it can be viewed by another application. While such an option does provide a crude review mechanism, some users might not consider it acceptable for this purpose.

4.4 How an Origin Server Interprets the Cookie Header

A user agent returns much of the information in the Set-Cookie header to the origin server when the Path attribute matches that of a new request. When it receives a Cookie header, the origin server should treat cookies with NAMEs whose prefix is \$ specially, as an attribute for the adjacent cookie. The value for such a NAME is to be interpreted as applying to the lexically (left-to-right) most recent cookie whose name does not have the \$ prefix. If there is no previous cookie, the value applies to the cookie mechanism as a whole. For example, consider the cookie

```
Cookie: $Version="1"; Customer="WILE_E_COYOTE";  
       $Path="/acme"
```

\$Version applies to the cookie mechanism as a whole (and gives the version number for the cookie mechanism). \$Path is an attribute whose value (/acme) defines the Path attribute that was used when the Customer cookie was defined in a Set-Cookie response header.

4.5 Caching Proxy Role

One reason for separating state information from both a URL and document content is to facilitate the scaling that caching permits. To support cookies, a caching proxy must obey these rules already in the HTTP specification:

- * Honor requests from the cache, if possible, based on cache validity rules.
- * Pass along a Cookie request header in any request that the proxy must make of another server.
- * Return the response to the client. Include any Set-Cookie response header.

- * Cache the received response subject to the control of the usual headers, such as Expires, Cache-control: no-cache, and Cache-control: private,
- * Cache the Set-Cookie subject to the control of the usual header, Cache-control: no-cache="set-cookie". (The Set-Cookie header should usually not be cached.)

Proxies must not introduce Set-Cookie (Cookie) headers of their own in proxy responses (requests).

5. EXAMPLES

5.1 Example 1

Most detail of request and response headers has been omitted. Assume the user agent has no stored cookies.

1. User Agent -> Server

```
POST /acme/login HTTP/1.1
[form data]
```

User identifies self via a form.

2. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie: Customer="WILE_E_COYOTE"; Version="1"; Path="/acme"
```

Cookie reflects user's identity.

3. User Agent -> Server

```
POST /acme/pickitem HTTP/1.1
Cookie: $Version="1"; Customer="WILE_E_COYOTE"; $Path="/acme"
[form data]
```

User selects an item for "shopping basket."

4. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie: Part_Number="Rocket_Launcher_0001"; Version="1";
           Path="/acme"
```

Shopping basket contains an item.

5. User Agent -> Server

```
POST /acme/shipping HTTP/1.1
Cookie: $Version="1";
       Customer="WILE_E_COYOTE"; $Path="/acme";
       Part_Number="Rocket_Launcher_0001"; $Path="/acme"
[form data]
```

User selects shipping method from form.

6. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie: Shipping="FedEx"; Version="1"; Path="/acme"
```

New cookie reflects shipping method.

7. User Agent -> Server

```
POST /acme/process HTTP/1.1
Cookie: $Version="1";
       Customer="WILE_E_COYOTE"; $Path="/acme";
       Part_Number="Rocket_Launcher_0001"; $Path="/acme";
       Shipping="FedEx"; $Path="/acme"
[form data]
```

User chooses to process order.

8. Server -> User Agent

```
HTTP/1.1 200 OK

Transaction is complete.
```

The user agent makes a series of requests on the origin server, after each of which it receives a new cookie. All the cookies have the same Path attribute and (default) domain. Because the request URLs all have /acme as a prefix, and that matches the Path attribute, each request contains all the cookies received so far.

5.2 Example 2

This example illustrates the effect of the Path attribute. All detail of request and response headers has been omitted. Assume the user agent has no stored cookies.

Imagine the user agent has received, in response to earlier requests, the response headers

```
Set-Cookie: Part_Number="Rocket_Launcher_0001"; Version="1";
           Path="/acme"
```

and

```
Set-Cookie: Part_Number="Riding_Rocket_0023"; Version="1";
           Path="/acme/ammo"
```

A subsequent request by the user agent to the (same) server for URLs of the form /acme/ammo/... would include the following request header:

```
Cookie: $Version="1";
       Part_Number="Riding_Rocket_0023"; $Path="/acme/ammo";
       Part_Number="Rocket_Launcher_0001"; $Path="/acme"
```

Note that the NAME=VALUE pair for the cookie with the more specific Path attribute, /acme/ammo, comes before the one with the less specific Path attribute, /acme. Further note that the same cookie name appears more than once.

A subsequent request by the user agent to the (same) server for a URL of the form /acme/parts/ would include the following request header:

Cookie: \$Version="1"; Part_Number="Rocket_Launcher_0001"; \$Path="/acme"

Here, the second cookie's Path attribute /acme/ammo is not a prefix of the request URL, /acme/parts/, so the cookie does not get forwarded to the server.

6. IMPLEMENTATION CONSIDERATIONS

Here we speculate on likely or desirable details for an origin server that implements state management.

6.1 Set-Cookie Content

An origin server's content should probably be divided into disjoint application areas, some of which require the use of state information. The application areas can be distinguished by their request URLs. The Set-Cookie header can incorporate information about the application areas by setting the Path attribute for each one.

The session information can obviously be clear or encoded text that describes state. However, if it grows too large, it can become unwieldy. Therefore, an implementor might choose for the session information to be a key to a server-side resource. Of course, using

a database creates some problems that this state management specification was meant to avoid, namely:

1. keeping real state on the server side;
2. how and when to garbage-collect the database entry, in case the user agent terminates the session by, for example, exiting.

6.2 Stateless Pages

Caching benefits the scalability of WWW. Therefore it is important to reduce the number of documents that have state embedded in them inherently. For example, if a shopping-basket-style application always displays a user's current basket contents on each page, those pages cannot be cached, because each user's basket's contents would be different. On the other hand, if each page contains just a link that allows the user to "Look at My Shopping Basket", the page can be cached.

6.3 Implementation Limits

Practical user agent implementations have limits on the number and size of cookies that they can store. In general, user agents' cookie support should have no fixed limits. They should strive to store as many frequently-used cookies as possible. Furthermore, general-use user agents should provide each of the following minimum capabilities individually, although not necessarily simultaneously:

- * at least 300 cookies
- * at least 4096 bytes per cookie (as measured by the size of the characters that comprise the cookie non-terminal in the syntax description of the Set-Cookie header)

- * at least 20 cookies per unique host or domain name

User agents created for specific purposes or for limited-capacity devices should provide at least 20 cookies of 4096 bytes, to ensure that the user can interact with a session-based origin server.

The information in a Set-Cookie response header must be retained in its entirety. If for some reason there is inadequate space to store the cookie, it must be discarded, not truncated.

Applications should use as few and as small cookies as possible, and they should cope gracefully with the loss of a cookie.

6.3.1 Denial of Service Attacks

User agents may choose to set an upper bound on the number of cookies to be stored from a given host or domain name or on the size of the cookie information. Otherwise a malicious server could attempt to flood a user agent with many cookies, or large cookies, on successive responses, which would force out cookies the user agent had received from other servers. However, the minima specified above should still be supported.

7. PRIVACY

7.1 User Agent Control

An origin server could create a Set-Cookie header to track the path of a user through the server. Users may object to this behavior as an intrusive accumulation of information, even if their identity is not evident. (Identity might become evident if a user subsequently fills out a form that contains identifying information.) This state management specification therefore requires that a user agent give the user control over such a possible intrusion, although the interface through which the user is given this control is left unspecified. However, the control mechanisms provided shall at least allow the user

- * to completely disable the sending and saving of cookies.
- * to determine whether a stateful session is in progress.
- * to control the saving of a cookie on the basis of the cookie's Domain attribute.

Such control could be provided by, for example, mechanisms

- * to notify the user when the user agent is about to send a cookie to the origin server, offering the option not to begin a session.
- * to display a visual indication that a stateful session is in progress.
- * to let the user decide which cookies, if any, should be saved when the user concludes a window or user agent session.
- * to let the user examine the contents of a cookie at any time.

A user agent usually begins execution with no remembered state information. It should be possible to configure a user agent never

to send Cookie headers, in which case it can never sustain state with an origin server. (The user agent would then behave like one that is unaware of how to handle Set-Cookie response headers.)

When the user agent terminates execution, it should let the user discard all state information. Alternatively, the user agent may ask the user whether state information should be retained; the default should be "no". If the user chooses to retain state information, it would be restored the next time the user agent runs.

NOTE: User agents should probably be cautious about using files to store cookies long-term. If a user runs more than one instance of the user agent, the cookies could be commingled or otherwise messed up.

7.2 Protocol Design

The restrictions on the value of the Domain attribute, and the rules concerning unverifiable transactions, are meant to reduce the ways that cookies can "leak" to the "wrong" site. The intent is to restrict cookies to one, or a closely related set of hosts. Therefore a request-host is limited as to what values it can set for Domain. We consider it acceptable for hosts host1.foo.com and host2.foo.com to share cookies, but not a.com and b.com.

Similarly, a server can only set a Path for cookies that are related to the request-URI.

8. SECURITY CONSIDERATIONS

8.1 Clear Text

The information in the Set-Cookie and Cookie headers is unprotected. Two consequences are:

1. Any sensitive information that is conveyed in them is exposed to intruders.
2. A malicious intermediary could alter the headers as they travel in either direction, with unpredictable results.

These facts imply that information of a personal and/or financial nature should only be sent over a secure channel. For less sensitive information, or when the content of the header is a database key, an origin server should be vigilant to prevent a bad Cookie value from causing failures.

8.2 Cookie Spoofing

Proper application design can avoid spoofing attacks from related domains. Consider:

1. User agent makes request to victim.cracker.edu, gets back cookie session_id="1234" and sets the default domain victim.cracker.edu.
2. User agent makes request to spoof.cracker.edu, gets back cookie session-id="1111", with Domain=".cracker.edu".

3. User agent makes request to victim.cracker.edu again, and passes

```
Cookie: $Version="1";  
        session_id="1234";  
        session_id="1111"; $Domain=".cracker.edu"
```

The server at victim.cracker.edu should detect that the second cookie was not one it originated by noticing that the Domain attribute is not for itself and ignore it.

8.3 Unexpected Cookie Sharing

A user agent should make every attempt to prevent the sharing of session information between hosts that are in different domains. Embedded or inlined objects may cause particularly severe privacy problems if they can be used to share cookies between disparate hosts. For example, a malicious server could embed cookie information for host a.com in a URI for a CGI on host b.com. User agent implementors are strongly encouraged to prevent this sort of exchange whenever possible.

9. OTHER, SIMILAR, PROPOSALS

Three other proposals have been made to accomplish similar goals. This specification is an amalgam of Kristol's State-Info proposal and Netscape's Cookie proposal.

Brian Behlendorf proposed a Session-ID header that would be user-agent-initiated and could be used by an origin server to track "clicktrails". It would not carry any origin-server-defined state, however. Phillip Hallam-Baker has proposed another client-defined session ID mechanism for similar purposes.

While both session IDs and cookies can provide a way to sustain stateful sessions, their intended purpose is different, and, consequently, the privacy requirements for them are different. A user initiates session IDs to allow servers to track progress through them, or to distinguish multiple users on a shared machine. Cookies are server-initiated, so the cookie mechanism described here gives users control over something that would otherwise take place without the users' awareness. Furthermore, cookies convey rich, server-selected information, whereas session IDs comprise user-selected, simple information.

10. HISTORICAL

10.1 Compatibility With Netscape's Implementation

HTTP/1.0 clients and servers may use Set-Cookie and Cookie headers that reflect Netscape's original cookie proposal. These notes cover inter-operation between "old" and "new" cookies.

10.1.1 Extended Cookie Header

This proposal adds attribute-value pairs to the Cookie request header in a compatible way. An "old" client that receives a "new" cookie will ignore attributes it does not understand; it returns what it does understand to the origin server. A "new" client always sends cookies in the new form.

An "old" server that receives a "new" cookie will see what it thinks are many cookies with names that begin with a \$, and it will ignore them. (The "old" server expects these cookies to be separated by semi-colon, not comma.) A "new" server can detect cookies that have passed through an "old" client, because they lack a \$Version attribute.

10.1.2 Expires and Max-Age

Netscape's original proposal defined an Expires header that took a date value in a fixed-length variant format in place of Max-Age:

Wdy, DD-Mon-YY HH:MM:SS GMT

Note that the Expires date format contains embedded spaces, and that "old" cookies did not have quotes around values. Clients that implement to this specification should be aware of "old" cookies and Expires.

10.1.3 Punctuation

In Netscape's original proposal, the values in attribute-value pairs did not accept "-quoted strings. Origin servers should be cautious about sending values that require quotes unless they know the receiving user agent understands them (i.e., "new" cookies). A ("new") user agent should only use quotes around values in Cookie headers when the cookie's version(s) is (are) all compliant with this specification or later.

In Netscape's original proposal, no whitespace was permitted around the = that separates attribute-value pairs. Therefore such whitespace should be used with caution in new implementations.

10.2 Caching and HTTP/1.0

Some caches, such as those conforming to HTTP/1.0, will inevitably cache the Set-Cookie header, because there was no mechanism to suppress caching of headers prior to HTTP/1.1. This caching can lead to security problems. Documents transmitted by an origin server along with Set-Cookie headers will usually either be uncacheable, or will be "pre-expired". As long as caches obey instructions not to cache documents (following Expires: <a date in the past> or Pragma: no-cache (HTTP/1.0), or Cache-control: no-cache (HTTP/1.1)) uncacheable documents present no problem. However, pre-expired documents may be stored in caches. They require validation (a conditional GET) on each new request, but some cache operators loosen the rules for their caches, and sometimes serve expired documents without first validating them. This combination of factors can lead to cookies meant for one user later being sent to another user. The Set-Cookie header is stored in the cache, and, although the document is stale (expired), the cache returns the document in response to later requests, including cached headers.

11. ACKNOWLEDGEMENTS

This document really represents the collective efforts of the following people, in addition to the authors: Roy Fielding, Marc Hedlund, Ted Hardie, Koen Holtman, Shel Kaphan, Rohit Khare.

12. AUTHORS' ADDRESSES

David M. Kristol
Bell Laboratories, Lucent Technologies
600 Mountain Ave. Room 2A-227
Murray Hill, NJ 07974

Phone: (908) 582-2250
Fax: (908) 582-5809
EMail: dmk@bell-labs.com

Lou Montulli
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043

Phone: (415) 528-2600
EMail: montulli@netscape.com

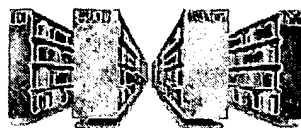
[Comment on RFC 2109](#)

Previous: [RFC 2108 - Definitions of
Managed Objects for IEEE 802.3 Repeater
Devices using SMIPv2](#)

Next: [RFC 2110 - MIME E-mail
Encapsulation of Aggregate Documents,
such as HTML \(MHTML\)](#)

[[RFC Index](#) | [RFC Search](#) | [Usenet FAQs](#) | [Web FAQs](#) | [Documents](#) | [Cities](#)]

APPENDIX II. M.



RFC 2965 (RFC2965)

Internet RFC/STD/FYI/BCP Archives

[[RFC Index](#) | [RFC Search](#) | [Usenet FAQs](#) | [Web FAQs](#) | [Documents](#) | [Cities](#)]

Alternate Formats: [rfc2965.txt](#) | [rfc2965.txt.pdf](#)

[Comment on RFC 2965](#)

RFC 2965 - HTTP State Management Mechanism

Network Working Group
Request for Comments: 2965
Obsoletes: 2109
Category: Standards Track

D. Kristol
Bell Laboratories, Lucent Technologies
L. Montulli
Epinions.com, Inc.
October 2000

HTTP State Management Mechanism

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

IESG Note

The IESG notes that this mechanism makes use of the .local top-level domain (TLD) internally when handling host names that don't contain any dots, and that this mechanism might not work in the expected way should an actual .local TLD ever be registered.

Abstract

This document specifies a way to create a stateful session with Hypertext Transfer Protocol (HTTP) requests and responses. It describes three new headers, Cookie, Cookie2, and Set-Cookie2, which carry state information between participating origin servers and user agents. The method described here differs from Netscape's Cookie proposal [Netscape], but it can interoperate with HTTP/1.0 user agents that use Netscape's method. (See the HISTORICAL section.)

This document reflects implementation experience with RFC 2109 and obsoletes it.

1. TERMINOLOGY

The terms user agent, client, server, proxy, origin server, and http_URL have the same meaning as in the HTTP/1.1 specification [RFC2616]. The terms abs_path and absoluteURI have the same meaning as in the URI Syntax specification [RFC2396].

Host name (HN) means either the host domain name (HDN) or the numeric Internet Protocol (IP) address of a host. The fully qualified domain name is preferred; use of numeric IP addresses is strongly discouraged.

The terms request-host and request-URI refer to the values the client would send to the server as, respectively, the host (but not port) and abs_path portions of the absoluteURI (http_URL) of the HTTP request line. Note that request-host is a HN.

The term effective host name is related to host name. If a host name contains no dots, the effective host name is that name with the string .local appended to it. Otherwise the effective host name is the same as the host name. Note that all effective host names contain at least one dot.

The term request-port refers to the port portion of the absoluteURI (http_URL) of the HTTP request line. If the absoluteURI has no explicit port, the request-port is the HTTP default, 80. The request-port of a cookie is the request-port of the request in which a Set-Cookie2 response header was returned to the user agent.

Host names can be specified either as an IP address or a HDN string. Sometimes we compare one host name with another. (Such comparisons SHALL be case-insensitive.) Host A's name domain-matches host B's if

- * their host name strings string-compare equal; or
- * A is a HDN string and has the form NB, where N is a non-empty name string; B has the form .B', and B' is a HDN string. (So, x.y.com domain-matches .Y.com but not Y.com.)

Note that domain-match is not a commutative operation: a.b.c.com domain-matches .c.com, but not the reverse.

The reach R of a host name H is defined as follows:

- * If
 - H is the host domain name of a host; and,
 - H has the form A.B; and
 - A has no embedded (that is, interior) dots; and
 - B has at least one embedded dot, or B is the string "local". then the reach of H is .B.
- * Otherwise, the reach of H is H.

For two strings that represent paths, P1 and P2, P1 path-matches P2 if P2 is a prefix of P1 (including the case where P1 and P2 string-compare equal). Thus, the string /tec/waldo path-matches /tec.

Because it was used in Netscape's original implementation of state management, we will use the term cookie to refer to the state information that passes between an origin server and user agent, and that gets stored by the user agent.

1.1 Requirements

The key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. STATE AND SESSIONS

This document describes a way to create stateful sessions with HTTP requests and responses. Currently, HTTP servers respond to each client request without relating that request to previous or subsequent requests; the state management mechanism allows clients and servers that wish to exchange state information to place HTTP requests and responses within a larger context, which we term a "session". This context might be used to create, for example, a "shopping cart", in which user selections can be aggregated before purchase, or a magazine browsing system, in which a user's previous reading affects which offerings are presented.

Neither clients nor servers are required to support cookies. A server MAY refuse to provide content to a client that does not return the cookies it sends.

3. DESCRIPTION

We describe here a way for an origin server to send state information to the user agent, and for the user agent to return the state information to the origin server. The goal is to have a minimal impact on HTTP and user agents.

3.1 Syntax: General

The two state management headers, Set-Cookie2 and Cookie, have common syntactic properties involving attribute-value pairs. The following grammar uses the notation, and tokens DIGIT (decimal digits), token

(informally, a sequence of non-special, non-white space characters), and http_URL from the HTTP/1.1 specification [RFC2616] to describe their syntax.

```
av-pairs    =    av-pair *(";" av-pair)
av-pair     =    attr ["=" value]           ; optional value
attr        =    token
value       =    token | quoted-string
```

Attributes (names) (attr) are case-insensitive. White space is permitted between tokens. Note that while the above syntax description shows value as optional, most attrs require them.

NOTE: The syntax above allows whitespace between the attribute and

the = sign.

3.2 Origin Server Role

3.2.1 General The origin server initiates a session, if it so desires. To do so, it returns an extra response header to the client, Set-Cookie2. (The details follow later.)

A user agent returns a Cookie request header (see below) to the origin server if it chooses to continue a session. The origin server MAY ignore it or use it to determine the current state of the session. It MAY send back to the client a Set-Cookie2 response header with the same or different information, or it MAY send no Set-Cookie2 header at all. The origin server effectively ends a session by sending the client a Set-Cookie2 header with Max-Age=0.

Servers MAY return Set-Cookie2 response headers with any response. User agents SHOULD send Cookie request headers, subject to other rules detailed below, with every request.

An origin server MAY include multiple Set-Cookie2 headers in a response. Note that an intervening gateway could fold multiple such headers into a single header.

3.2.2 Set-Cookie2 Syntax The syntax for the Set-Cookie2 response header is

```

set-cookie      =      "Set-Cookie2:" cookies
cookies         =      1#cookie
cookie          =      NAME "=" VALUE *("; " set-cookie-av)
NAME            =      attr
VALUE          =      value
set-cookie-av   =      "Comment" "=" value
                  |      "CommentURL" "=" <"> http_URL <">
                  |      "Discard"
                  |      "Domain" "=" value
                  |      "Max-Age" "=" value
                  |      "Path" "=" value
                  |      "Port" [ "=" <"> portlist <"> ]
                  |      "Secure"
                  |      "Version" "=" 1*DIGIT
portlist        =      1#portnum
portnum         =      1*DIGIT

```

Informally, the Set-Cookie2 response header comprises the token Set-Cookie2:, followed by a comma-separated list of one or more cookies. Each cookie begins with a NAME=VALUE pair, followed by zero or more semi-colon-separated attribute-value pairs. The syntax for attribute-value pairs was shown earlier. The specific attributes and the semantics of their values follows. The NAME=VALUE attribute-value pair MUST come first in each cookie. The others, if present, can occur in any order. If an attribute appears more than once in a cookie, the client SHALL use only the value associated with the first appearance of the attribute; a client MUST ignore values after the first.

The NAME of a cookie MAY be the same as one of the attributes in this specification. However, because the cookie's NAME must come first in a Set-Cookie2 response header, the NAME and its VALUE cannot be confused with an attribute-value pair.

NAME=VALUE

REQUIRED. The name of the state information ("cookie") is NAME, and its value is VALUE. NAMES that begin with \$ are reserved and MUST NOT be used by applications.

The VALUE is opaque to the user agent and may be anything the origin server chooses to send, possibly in a server-selected printable ASCII encoding. "Opaque" implies that the content is of interest and relevance only to the origin server. The content may, in fact, be readable by anyone that examines the Set-Cookie2 header.

Comment=value

OPTIONAL. Because cookies can be used to derive or store private information about a user, the value of the Comment attribute allows an origin server to document how it intends to use the cookie. The user can inspect the information to decide whether to initiate or continue a session with this cookie. Characters in value MUST be in UTF-8 encoding. [RFC2279]

CommentURL="http_URL"

OPTIONAL. Because cookies can be used to derive or store private information about a user, the CommentURL attribute allows an origin server to document how it intends to use the cookie. The user can inspect the information identified by the URL to decide whether to initiate or continue a session with this cookie.

Discard

OPTIONAL. The Discard attribute instructs the user agent to discard the cookie unconditionally when the user agent terminates.

Domain=value

OPTIONAL. The value of the Domain attribute specifies the domain for which the cookie is valid. If an explicitly specified value does not start with a dot, the user agent supplies a leading dot.

Max-Age=value

OPTIONAL. The value of the Max-Age attribute is delta-seconds, the lifetime of the cookie in seconds, a decimal non-negative integer. To handle cached cookies correctly, a client SHOULD calculate the age of the cookie according to the age calculation rules in the HTTP/1.1 specification [RFC2616]. When the age is greater than delta-seconds seconds, the client SHOULD discard the cookie. A value of zero means the cookie SHOULD be discarded immediately.

Path=value

OPTIONAL. The value of the Path attribute specifies the subset of URLs on the origin server to which this cookie applies.

Port["portlist"]

OPTIONAL. The Port attribute restricts the port to which a cookie may be returned in a Cookie request header. Note that the syntax REQUIRES quotes around the OPTIONAL portlist even if there is only one portnum in portlist.

Secure

OPTIONAL. The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin

server whenever it sends back this cookie, to protect the confidentiality and authenticity of the information in the cookie.

The user agent (possibly with user interaction) MAY determine what level of security it considers appropriate for "secure" cookies. The Secure attribute should be considered security advice from the server to the user agent, indicating that it is in the session's interest to protect the cookie contents. When it sends a "secure" cookie back to a server, the user agent SHOULD use no less than the same level of security as was used when it received the cookie from the server.

Version=value

REQUIRED. The value of the Version attribute, a decimal integer, identifies the version of the state management specification to which the cookie conforms. For this specification, Version=1 applies.

3.2.3 Controlling Caching An origin server must be cognizant of the effect of possible caching of both the returned resource and the Set-Cookie2 header. Caching "public" documents is desirable. For example, if the origin server wants to use a public document such as a "front door" page as a sentinel to indicate the beginning of a session for which a Set-Cookie2 response header must be generated, the page SHOULD be stored in caches "pre-expired" so that the origin server will see further requests. "Private documents", for example those that contain information strictly private to a session, SHOULD NOT be cached in shared caches.

If the cookie is intended for use by a single user, the Set-Cookie2 header SHOULD NOT be cached. A Set-Cookie2 header that is intended to be shared by multiple users MAY be cached.

The origin server SHOULD send the following additional HTTP/1.1 response headers, depending on circumstances:

- * To suppress caching of the Set-Cookie2 header:

Cache-control: no-cache="set-cookie2"

and one of the following:

- * To suppress caching of a private document in shared caches:

Cache-control: private

- * To allow caching of a document and require that it be validated before returning it to the client:

Cache-Control: must-revalidate, max-age=0

- * To allow caching of a document, but to require that proxy caches (not user agent caches) validate it before returning it to the client:

Cache-Control: proxy-revalidate, max-age=0

- * To allow caching of a document and request that it be validated before returning it to the client (by "pre-expiring" it):

Cache-control: max-age=0

Not all caches will revalidate the document in every case.

HTTP/1.1 servers MUST send Expires: old-date (where old-date is a date long in the past) on responses containing Set-Cookie2 response headers unless they know for certain (by out of band means) that there are no HTTP/1.0 proxies in the response chain. HTTP/1.1 servers MAY send other Cache-Control directives that permit caching by HTTP/1.1 proxies in addition to the Expires: old-date directive; the Cache-Control directive will override the Expires: old-date for HTTP/1.1 proxies.

3.3 User Agent Role

3.3.1 Interpreting Set-Cookie2 The user agent keeps separate track of state information that arrives via Set-Cookie2 response headers from each origin server (as distinguished by name or IP address and port). The user agent MUST ignore attribute-value pairs whose attribute it does not recognize. The user agent applies these defaults for optional attributes that are missing:

Discard The default behavior is dictated by the presence or absence of a Max-Age attribute.

Domain Defaults to the effective request-host. (Note that because there is no dot at the beginning of effective request-host, the default Domain can only domain-match itself.)

Max-Age The default behavior is to discard the cookie when the user agent exits.

Path Defaults to the path of the request URL that generated the Set-Cookie2 response, up to and including the right-most /.

Port The default behavior is that a cookie MAY be returned to any request-port.

Secure If absent, the user agent MAY send the cookie over an insecure channel.

3.3.2 Rejecting Cookies To prevent possible security or privacy violations, a user agent rejects a cookie according to rules below. The goal of the rules is to try to limit the set of servers for which a cookie is valid, based on the values of the Path, Domain, and Port attributes and the request-URI, request-host and request-port.

A user agent rejects (SHALL NOT store its information) if the Version attribute is missing. Moreover, a user agent rejects (SHALL NOT store its information) if any of the following is true of the attributes explicitly present in the Set-Cookie2 response header:

- * The value for the Path attribute is not a prefix of the request-URI.
- * The value for the Domain attribute contains no embedded dots, and the value is not .local.
- * The effective host name that derives from the request-host does not domain-match the Domain attribute.

- * The request-host is a HDN (not IP address) and has the form HD, where D is the value of the Domain attribute, and H is a string that contains one or more dots.
- * The Port attribute has a "port-list", and the request-port was not in the list.

Examples:

- * A Set-Cookie2 from request-host y.x.foo.com for Domain=.foo.com would be rejected, because H is y.x and contains a dot.
- * A Set-Cookie2 from request-host x.foo.com for Domain=.foo.com would be accepted.
- * A Set-Cookie2 with Domain=.com or Domain=.com., will always be rejected, because there is no embedded dot.
- * A Set-Cookie2 with Domain=ajax.com will be accepted, and the value for Domain will be taken to be .ajax.com, because a dot gets prepended to the value.
- * A Set-Cookie2 with Port="80,8000" will be accepted if the request was made to port 80 or 8000 and will be rejected otherwise.
- * A Set-Cookie2 from request-host example for Domain=.local will be accepted, because the effective host name for the request-host is example.local, and example.local domain-matches .local.

3.3.3 Cookie Management If a user agent receives a Set-Cookie2 response header whose NAME is the same as that of a cookie it has previously stored, the new cookie supersedes the old when: the old and new Domain attribute values compare equal, using a case-insensitive string-compare; and, the old and new Path attribute values string-compare equal (case-sensitive). However, if the Set-Cookie2 has a value for Max-Age of zero, the (old and new) cookie is discarded. Otherwise a cookie persists (resources permitting) until whichever happens first, then gets discarded: its Max-Age lifetime is exceeded; or, if the Discard attribute is set, the user agent terminates the session.

Because user agents have finite space in which to store cookies, they MAY also discard older cookies to make space for newer ones, using, for example, a least-recently-used algorithm, along with constraints on the maximum number of cookies that each origin server may set.

If a Set-Cookie2 response header includes a Comment attribute, the user agent SHOULD store that information in a human-readable form with the cookie and SHOULD display the comment text as part of a cookie inspection user interface.

If a Set-Cookie2 response header includes a CommentURL attribute, the user agent SHOULD store that information in a human-readable form with the cookie, or, preferably, SHOULD allow the user to follow the http_URL link as part of a cookie inspection user interface.

The cookie inspection user interface may include a facility whereby a user can decide, at the time the user agent receives the Set-Cookie2

response header, whether or not to accept the cookie. A potentially confusing situation could arise if the following sequence occurs:

- * the user agent receives a cookie that contains a CommentURL attribute;
- * the user agent's cookie inspection interface is configured so that it presents a dialog to the user before the user agent accepts the cookie;
- * the dialog allows the user to follow the CommentURL link when the user agent receives the cookie; and,
- * when the user follows the CommentURL link, the origin server (or another server, via other links in the returned content) returns another cookie.

The user agent SHOULD NOT send any cookies in this context. The user agent MAY discard any cookie it receives in this context that the user has not, through some user agent mechanism, deemed acceptable.

User agents SHOULD allow the user to control cookie destruction, but they MUST NOT extend the cookie's lifetime beyond that controlled by the Discard and Max-Age attributes. An infrequently-used cookie may function as a "preferences file" for network applications, and a user may wish to keep it even if it is the least-recently-used cookie. One possible implementation would be an interface that allows the permanent storage of a cookie through a checkbox (or, conversely, its immediate destruction).

Privacy considerations dictate that the user have considerable control over cookie management. The PRIVACY section contains more information.

3.3.4 Sending Cookies to the Origin Server When it sends a request to an origin server, the user agent includes a Cookie request header if it has stored cookies that are applicable to the request, based on

- * the request-host and request-port;
- * the request-URI;
- * the cookie's age.

The syntax for the header is:

```

cookie           = "Cookie:" cookie-version 1*("(";" | ","") cookie-value)
cookie-value     = NAME "=" VALUE [";" path] [";" domain] [";" port]
cookie-version   = "$Version" "=" value
NAME             = attr
VALUE            = value
path             = "$Path" "=" value
domain           = "$Domain" "=" value
port             = "$Port" [ "=" "<"> value "<"> ]

```

The value of the cookie-version attribute MUST be the value from the Version attribute of the corresponding Set-Cookie2 response header. Otherwise the value for cookie-version is 0. The value for the path

attribute MUST be the value from the Path attribute, if one was

present, of the corresponding Set-Cookie2 response header. Otherwise the attribute SHOULD be omitted from the Cookie request header. The value for the domain attribute MUST be the value from the Domain attribute, if one was present, of the corresponding Set-Cookie2 response header. Otherwise the attribute SHOULD be omitted from the Cookie request header.

The port attribute of the Cookie request header MUST mirror the Port attribute, if one was present, in the corresponding Set-Cookie2 response header. That is, the port attribute MUST be present if the Port attribute was present in the Set-Cookie2 header, and it MUST have the same value, if any. Otherwise, if the Port attribute was absent from the Set-Cookie2 header, the attribute likewise MUST be omitted from the Cookie request header.

Note that there is neither a Comment nor a CommentURL attribute in the Cookie request header corresponding to the ones in the Set-Cookie2 response header. The user agent does not return the comment information to the origin server.

The user agent applies the following rules to choose applicable cookie-values to send in Cookie request headers from among all the cookies it has received.

Domain Selection

The origin server's effective host name MUST domain-match the Domain attribute of the cookie.

Port Selection

There are three possible behaviors, depending on the Port attribute in the Set-Cookie2 response header:

1. By default (no Port attribute), the cookie MAY be sent to any port.
2. If the attribute is present but has no value (e.g., Port), the cookie MUST only be sent to the request-port it was received from.
3. If the attribute has a port-list, the cookie MUST only be returned if the new request-port is one of those listed in port-list.

Path Selection

The request-URI MUST path-match the Path attribute of the cookie.

Max-Age Selection

Cookies that have expired should have been discarded and thus are not forwarded to an origin server.

If multiple cookies satisfy the criteria above, they are ordered in the Cookie header such that those with more specific Path attributes precede those with less specific. Ordering with respect to other attributes (e.g., Domain) is unspecified.

Note: For backward compatibility, the separator in the Cookie header is semi-colon (;) everywhere. A server SHOULD also accept comma (,) as the separator between cookie-values for future compatibility.

3.3.5 Identifying What Version is Understood: Cookie2 The Cookie2

request header facilitates interoperation between clients and servers that understand different versions of the cookie specification. When the client sends one or more cookies to an origin server, if at least one of those cookies contains a \$Version attribute whose value is different from the version that the client understands, then the client MUST also send a Cookie2 request header, the syntax for which is

```
cookie2 =      "Cookie2:" cookie-version
```

Here the value for cookie-version is the highest version of cookie specification (currently 1) that the client understands. The client needs to send at most one such request header per request.

3.3.6 Sending Cookies in Unverifiable Transactions Users MUST have control over sessions in order to ensure privacy. (See PRIVACY section below.) To simplify implementation and to prevent an additional layer of complexity where adequate safeguards exist, however, this document distinguishes between transactions that are verifiable and those that are unverifiable. A transaction is verifiable if the user, or a user-designated agent, has the option to review the request-URI prior to its use in the transaction. A transaction is unverifiable if the user does not have that option. Unverifiable transactions typically arise when a user agent automatically requests inlined or embedded entities or when it resolves redirection (3xx) responses from an origin server. Typically the origin transaction, the transaction that the user initiates, is verifiable, and that transaction may directly or indirectly induce the user agent to make unverifiable transactions.

An unverifiable transaction is to a third-party host if its request-host U does not domain-match the reach R of the request-host O in the origin transaction.

When it makes an unverifiable transaction, a user agent MUST disable all cookie processing (i.e., MUST NOT send cookies, and MUST NOT accept any received cookies) if the transaction is to a third-party host.

This restriction prevents a malicious service author from using unverifiable transactions to induce a user agent to start or continue a session with a server in a different domain. The starting or continuation of such sessions could be contrary to the privacy expectations of the user, and could also be a security problem.

User agents MAY offer configurable options that allow the user agent, or any autonomous programs that the user agent executes, to ignore the above rule, so long as these override options default to "off".

(N.B. Mechanisms may be proposed that will automate overriding the third-party restrictions under controlled conditions.)

Many current user agents already provide a review option that would render many links verifiable. For instance, some user agents display the URL that would be referenced for a particular link when the mouse pointer is placed over that link. The user can therefore determine whether to visit that site before causing the browser to do so.

(Though not implemented on current user agents, a similar technique could be used for a button used to submit a form -- the user agent could display the action to be taken if the user were to select that

button.) However, even this would not make all links verifiable; for example, links to automatically loaded images would not normally be subject to "mouse pointer" verification.

Many user agents also provide the option for a user to view the HTML source of a document, or to save the source to an external file where it can be viewed by another application. While such an option does provide a crude review mechanism, some users might not consider it acceptable for this purpose.

3.4 How an Origin Server Interprets the Cookie Header

A user agent returns much of the information in the Set-Cookie2 header to the origin server when the request-URI path-matches the Path attribute of the cookie. When it receives a Cookie header, the origin server SHOULD treat cookies with NAMES whose prefix is \$ specially, as an attribute for the cookie.

3.5 Caching Proxy Role

One reason for separating state information from both a URL and document content is to facilitate the scaling that caching permits. To support cookies, a caching proxy MUST obey these rules already in the HTTP specification:

- * Honor requests from the cache, if possible, based on cache validity rules.
- * Pass along a Cookie request header in any request that the proxy must make of another server.
- * Return the response to the client. Include any Set-Cookie2 response header.
- * Cache the received response subject to the control of the usual headers, such as Expires,

Cache-control: no-cache

and

Cache-control: private

- * Cache the Set-Cookie2 subject to the control of the usual header,

Cache-control: no-cache="set-cookie2"

(The Set-Cookie2 header should usually not be cached.)

Proxies MUST NOT introduce Set-Cookie2 (Cookie) headers of their own in proxy responses (requests).

4. EXAMPLES

4.1 Example 1

Most detail of request and response headers has been omitted. Assume the user agent has no stored cookies.

1. User Agent -> Server

```
POST /acme/login HTTP/1.1
[form data]
```

User identifies self via a form.

2. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie2: Customer="WILE_E_COYOTE"; Version="1"; Path="/acme"
```

Cookie reflects user's identity.

3. User Agent -> Server

```
POST /acme/pickitem HTTP/1.1
Cookie: $Version="1"; Customer="WILE_E_COYOTE"; $Path="/acme"
[form data]
```

User selects an item for "shopping basket".

4. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie2: Part_Number="Rocket_Launcher_0001"; Version="1";
             Path="/acme"
```

Shopping basket contains an item.

5. User Agent -> Server

```
POST /acme/shipping HTTP/1.1
Cookie: $Version="1";
       Customer="WILE_E_COYOTE"; $Path="/acme";
       Part_Number="Rocket_Launcher_0001"; $Path="/acme"
[form data]
```

User selects shipping method from form.

6. Server -> User Agent

```
HTTP/1.1 200 OK
Set-Cookie2: Shipping="FedEx"; Version="1"; Path="/acme"
```

New cookie reflects shipping method.

7. User Agent -> Server

```
POST /acme/process HTTP/1.1
Cookie: $Version="1";
       Customer="WILE_E_COYOTE"; $Path="/acme";
       Part_Number="Rocket_Launcher_0001"; $Path="/acme";
       Shipping="FedEx"; $Path="/acme"
[form data]
```

User chooses to process order.

8. Server -> User Agent

HTTP/1.1 200 OK

Transaction is complete.

The user agent makes a series of requests on the origin server, after each of which it receives a new cookie. All the cookies have the same Path attribute and (default) domain. Because the request-URIs all path-match /acme, the Path attribute of each cookie, each request contains all the cookies received so far.

4.2 Example 2

This example illustrates the effect of the Path attribute. All detail of request and response headers has been omitted. Assume the user agent has no stored cookies.

Imagine the user agent has received, in response to earlier requests, the response headers

```
Set-Cookie2: Part_Number="Rocket_Launcher_0001"; Version="1";  
             Path="/acme"
```

and

```
Set-Cookie2: Part_Number="Riding_Rocket_0023"; Version="1";  
             Path="/acme/ammo"
```

A subsequent request by the user agent to the (same) server for URLs of the form /acme/ammo/... would include the following request header:

```
Cookie: $Version="1";  
        Part_Number="Riding_Rocket_0023"; $Path="/acme/ammo";  
        Part_Number="Rocket_Launcher_0001"; $Path="/acme"
```

Note that the NAME=VALUE pair for the cookie with the more specific Path attribute, /acme/ammo, comes before the one with the less specific Path attribute, /acme. Further note that the same cookie name appears more than once.

A subsequent request by the user agent to the (same) server for a URL of the form /acme/parts/ would include the following request header:

```
Cookie: $Version="1"; Part_Number="Rocket_Launcher_0001";  
$Path="/acme"
```

Here, the second cookie's Path attribute /acme/ammo is not a prefix of the request URL, /acme/parts/, so the cookie does not get forwarded to the server.

5. IMPLEMENTATION CONSIDERATIONS

Here we provide guidance on likely or desirable details for an origin server that implements state management.

5.1 Set-Cookie2 Content

An origin server's content should probably be divided into disjoint application areas, some of which require the use of state information. The application areas can be distinguished by their

request URLs. The Set-Cookie2 header can incorporate information about the application areas by setting the Path attribute for each one.

The session information can obviously be clear or encoded text that describes state. However, if it grows too large, it can become unwieldy. Therefore, an implementor might choose for the session information to be a key to a server-side resource. Of course, using a database creates some problems that this state management specification was meant to avoid, namely:

1. keeping real state on the server side;
2. how and when to garbage-collect the database entry, in case the user agent terminates the session by, for example, exiting.

5.2 Stateless Pages

Caching benefits the scalability of WWW. Therefore it is important to reduce the number of documents that have state embedded in them inherently. For example, if a shopping-basket-style application always displays a user's current basket contents on each page, those pages cannot be cached, because each user's basket's contents would be different. On the other hand, if each page contains just a link that allows the user to "Look at My Shopping Basket", the page can be cached.

5.3 Implementation Limits

Practical user agent implementations have limits on the number and size of cookies that they can store. In general, user agents' cookie support should have no fixed limits. They should strive to store as many frequently-used cookies as possible. Furthermore, general-use user agents SHOULD provide each of the following minimum capabilities individually, although not necessarily simultaneously:

- * at least 300 cookies
- * at least 4096 bytes per cookie (as measured by the characters that comprise the cookie non-terminal in the syntax description of the Set-Cookie2 header, and as received in the Set-Cookie2 header)
- * at least 20 cookies per unique host or domain name

User agents created for specific purposes or for limited-capacity devices SHOULD provide at least 20 cookies of 4096 bytes, to ensure that the user can interact with a session-based origin server.

The information in a Set-Cookie2 response header MUST be retained in its entirety. If for some reason there is inadequate space to store the cookie, it MUST be discarded, not truncated.

Applications should use as few and as small cookies as possible, and they should cope gracefully with the loss of a cookie.

5.3.1 Denial of Service Attacks User agents MAY choose to set an upper bound on the number of cookies to be stored from a given host or domain name or on the size of the cookie information. Otherwise a malicious server could attempt to flood a user agent with many

cookies, or large cookies, on successive responses, which would force out cookies the user agent had received from other servers. However, the minima specified above SHOULD still be supported.

6. PRIVACY

Informed consent should guide the design of systems that use cookies. A user should be able to find out how a web site plans to use information in a cookie and should be able to choose whether or not those policies are acceptable. Both the user agent and the origin server must assist informed consent.

6.1 User Agent Control

An origin server could create a Set-Cookie2 header to track the path of a user through the server. Users may object to this behavior as an intrusive accumulation of information, even if their identity is not evident. (Identity might become evident, for example, if a user subsequently fills out a form that contains identifying information.) This state management specification therefore requires that a user agent give the user control over such a possible intrusion, although the interface through which the user is given this control is left unspecified. However, the control mechanisms provided SHALL at least allow the user

- * to completely disable the sending and saving of cookies.
- * to determine whether a stateful session is in progress.
- * to control the saving of a cookie on the basis of the cookie's Domain attribute.

Such control could be provided, for example, by mechanisms

- * to notify the user when the user agent is about to send a cookie to the origin server, to offer the option not to begin a session.
- * to display a visual indication that a stateful session is in progress.
- * to let the user decide which cookies, if any, should be saved when the user concludes a window or user agent session.
- * to let the user examine and delete the contents of a cookie at any time.

A user agent usually begins execution with no remembered state information. It SHOULD be possible to configure a user agent never to send Cookie headers, in which case it can never sustain state with an origin server. (The user agent would then behave like one that is unaware of how to handle Set-Cookie2 response headers.)

When the user agent terminates execution, it SHOULD let the user discard all state information. Alternatively, the user agent MAY ask the user whether state information should be retained; the default should be "no". If the user chooses to retain state information, it would be restored the next time the user agent runs.

NOTE: User agents should probably be cautious about using files to

store cookies long-term. If a user runs more than one instance of the user agent, the cookies could be commingled or otherwise corrupted.

6.2 Origin Server Role

An origin server SHOULD promote informed consent by adding CommentURL or Comment information to the cookies it sends. CommentURL is preferred because of the opportunity to provide richer information in a multiplicity of languages.

6.3 Clear Text

The information in the Set-Cookie2 and Cookie headers is unprotected. As a consequence:

1. Any sensitive information that is conveyed in them is exposed to intruders.
2. A malicious intermediary could alter the headers as they travel in either direction, with unpredictable results.

These facts imply that information of a personal and/or financial nature should only be sent over a secure channel. For less sensitive information, or when the content of the header is a database key, an origin server should be vigilant to prevent a bad Cookie value from causing failures.

A user agent in a shared user environment poses a further risk. Using a cookie inspection interface, User B could examine the contents of cookies that were saved when User A used the machine.

7. SECURITY CONSIDERATIONS

7.1 Protocol Design

The restrictions on the value of the Domain attribute, and the rules concerning unverifiable transactions, are meant to reduce the ways that cookies can "leak" to the "wrong" site. The intent is to restrict cookies to one host, or a closely related set of hosts. Therefore a request-host is limited as to what values it can set for Domain. We consider it acceptable for hosts host1.foo.com and host2.foo.com to share cookies, but not a.com and b.com.

Similarly, a server can set a Path only for cookies that are related to the request-URI.

7.2 Cookie Spoofing

Proper application design can avoid spoofing attacks from related domains. Consider:

1. User agent makes request to victim.cracker.edu, gets back cookie session_id="1234" and sets the default domain victim.cracker.edu.
2. User agent makes request to spoof.cracker.edu, gets back cookie session-id="1111", with Domain=".cracker.edu".
3. User agent makes request to victim.cracker.edu again, and

passes

```
Cookie: $Version="1"; session_id="1234",  
       $Version="1"; session_id="1111"; $Domain=".cracker.edu"
```

The server at victim.cracker.edu should detect that the second cookie was not one it originated by noticing that the Domain attribute is not for itself and ignore it.

7.3 Unexpected Cookie Sharing

A user agent SHOULD make every attempt to prevent the sharing of session information between hosts that are in different domains. Embedded or inlined objects may cause particularly severe privacy problems if they can be used to share cookies between disparate hosts. For example, a malicious server could embed cookie information for host a.com in a URI for a CGI on host b.com. User agent implementors are strongly encouraged to prevent this sort of exchange whenever possible.

7.4 Cookies For Account Information

While it is common practice to use them this way, cookies are not designed or intended to be used to hold authentication information, such as account names and passwords. Unless such cookies are exchanged over an encrypted path, the account information they contain is highly vulnerable to perusal and theft.

8. OTHER, SIMILAR, PROPOSALS

Apart from [RFC 2109](#), three other proposals have been made to accomplish similar goals. This specification began as an amalgam of Kristol's State-Info proposal [DMK95] and Netscape's Cookie proposal [Netscape].

Brian Behlendorf proposed a Session-ID header that would be user-agent-initiated and could be used by an origin server to track "clicktrails". It would not carry any origin-server-defined state, however. Phillip Hallam-Baker has proposed another client-defined session ID mechanism for similar purposes.

While both session IDs and cookies can provide a way to sustain stateful sessions, their intended purpose is different, and, consequently, the privacy requirements for them are different. A user initiates session IDs to allow servers to track progress through them, or to distinguish multiple users on a shared machine. Cookies are server-initiated, so the cookie mechanism described here gives users control over something that would otherwise take place without the users' awareness. Furthermore, cookies convey rich, server-selected information, whereas session IDs comprise user-selected, simple information.

9. HISTORICAL

9.1 Compatibility with Existing Implementations

Existing cookie implementations, based on the Netscape specification, use the Set-Cookie (not Set-Cookie2) header. User agents that receive in the same response both a Set-Cookie and Set-Cookie2 response header for the same cookie MUST discard the Set-Cookie

information and use only the Set-Cookie2 information. Furthermore, a user agent MUST assume, if it received a Set-Cookie2 response header, that the sending server complies with this document and will understand Cookie request headers that also follow this specification.

New cookies MUST replace both equivalent old- and new-style cookies. That is, if a user agent that follows both this specification and Netscape's original specification receives a Set-Cookie2 response header, and the NAME and the Domain and Path attributes match (per the Cookie Management section) a Netscape-style cookie, the Netscape-style cookie MUST be discarded, and the user agent MUST retain only the cookie adhering to this specification.

Older user agents that do not understand this specification, but that do understand Netscape's original specification, will not recognize the Set-Cookie2 response header and will receive and send cookies according to the older specification.

A user agent that supports both this specification and Netscape-style cookies SHOULD send a Cookie request header that follows the older Netscape specification if it received the cookie in a Set-Cookie response header and not in a Set-Cookie2 response header. However, it SHOULD send the following request header as well:

```
Cookie2: $Version="1"
```

The Cookie2 header advises the server that the user agent understands new-style cookies. If the server understands new-style cookies, as well, it SHOULD continue the stateful session by sending a Set-Cookie2 response header, rather than Set-Cookie. A server that does not understand new-style cookies will simply ignore the Cookie2 request header.

9.2 Caching and HTTP/1.0

Some caches, such as those conforming to HTTP/1.0, will inevitably cache the Set-Cookie2 and Set-Cookie headers, because there was no mechanism to suppress caching of headers prior to HTTP/1.1. This caching can lead to security problems. Documents transmitted by an origin server along with Set-Cookie2 and Set-Cookie headers usually either will be uncacheable, or will be "pre-expired". As long as caches obey instructions not to cache documents (following Expires: <a date in the past> or Pragma: no-cache (HTTP/1.0), or Cache-control: no-cache (HTTP/1.1)) uncacheable documents present no problem. However, pre-expired documents may be stored in caches. They require validation (a conditional GET) on each new request, but some cache operators loosen the rules for their caches, and sometimes serve expired documents without first validating them. This combination of factors can lead to cookies meant for one user later being sent to another user. The Set-Cookie2 and Set-Cookie headers are stored in the cache, and, although the document is stale (expired), the cache returns the document in response to later requests, including cached headers.

10. ACKNOWLEDGEMENTS

This document really represents the collective efforts of the HTTP Working Group of the IETF and, particularly, the following people, in addition to the authors: Roy Fielding, Yaron Goland, Marc Hedlund,

Ted Hardie, Koen Holtman, Shel Kaphan, Rohit Khare, Foteos Macrides,
David W. Morris.

11. AUTHORS' ADDRESSES

David M. Kristol
Bell Laboratories, Lucent Technologies
600 Mountain Ave. Room 2A-333
Murray Hill, NJ 07974

Phone: (908) 582-2250
Fax: (908) 582-1239
EMail: dmk@bell-labs.com

Lou Montulli
Epinions.com, Inc.
2037 Landings Dr.
Mountain View, CA 94301

EMail: lou@montulli.org

12. REFERENCES

- [DMK95] Kristol, D.M., "Proposed HTTP State-Info Mechanism", available at <http://portal.research.bell-labs.com/~dmk/state-info.html>, September, 1995.
- [Netscape] "Persistent Client State -- HTTP Cookies", available at http://www.netscape.com/newsref/std/cookie_spec.html, undated.
- [RFC2109] Kristol, D. and L. Montulli, "HTTP State Management Mechanism", [RFC 2109](#), February 1997.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.
- [RFC2279] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO-10646", [RFC 2279](#), January 1998.
- [RFC2396] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", [RFC 2396](#), August 1998.
- [RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", [RFC 2616](#), June 1999.

13. Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other

Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Comment on RFC 2965

Previous: [RFC 2964 - Use of HTTP State Management](#)

Next: [RFC 2966 - Domain-wide Prefix Distribution with Two-Level IS-IS](#)

[[RFC Index](#) | [RFC Search](#) | [Usenet FAQs](#) | [Web FAQs](#) | [Documents](#) | [Cities](#)]

APPENDIX II. N.

LEXSEE 857 F.2D 778

**UNITED STATES OF AMERICA, Plaintiff/Appellant, and ZIMMER, INC.,
Involuntary Plaintiff/Counterclaim-Defendant, v. TELELECTRONICS, INC. and BGS
MEDICAL, INC., Defendants/Counterclaim-Plaintiffs/Cross-Appellants**

Nos. 87-1445, 87-1446

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

857 F.2d 778; 1988 U.S. App. LEXIS 13542; 8 U.S.P.Q.2D (BNA) 1217

September 22, 1988, Decided

PRIOR HISTORY: [1]**

Appealed from: U.S. District Court for the District of Colorado, Judge Matsch.

LexisNexis(R) Headnotes

COUNSEL:

John Fargo, Assistant Director, Commercial Litigation Branch, Department of Justice, of Washington, District of Columbia, argued for Plaintiff/Appellant.

Michael I. Rackman, Gottlieb, Rackman & Reisman, P.C., of New York, New York, argued for Defendants/CounterClaim-Plaintiffs/Cross-Appellants. With him on the brief were Barry A. Cooper and Jeffery M. Kaden. Also on the brief was William C. Nealon, of Suffield, Connecticut, of Counsel.

JUDGES:

Newman, Archer and Mayer, Circuit Judges.

OPINIONBY:

ARCHER

OPINION:

[*779] ARCHER, Circuit Judge.

The United States of America (government) appeals the judgment of the United States District Court for the District of Colorado in *United States v. Telelectronics, Inc.*, 658 F. Supp. 579, 3 USPQ2d 1571 (D. Colo. 1987),

holding that Telelectronics, Inc. and BGS Medical, Inc. (Telelectronics) do not infringe U.S. Patent No. 3,842,841 ('841). Telelectronics cross-appeals the determinations that the '841 patent is not invalid under 35 U.S.C. § 112 (1982) and that Telelectronics is not entitled to attorney fees under [**2] 35 U.S.C. § 285 (1982). n1 We reverse the district court's holding that the '841 patent is not infringed by Telelectronics. The determinations that the patent is not invalid under section 112 and that Telelectronics is not entitled to attorney fees are affirmed.

n1 Telelectronics has not appealed the district court's holdings on other issues it raised below.

Background

The '841 patent issued to Carl T. Brighton, et al. and was assigned to the United States. The patent resulted from work under contract between the Office of Naval Research and the University of Pennsylvania, where the inventors were employed. 658 F. Supp. at 581, 3 USPQ2d at 1571. The '841 patent is directed to a bone growth stimulator device for speeding the healing of fractures and other bone defects. The accused devices of Telelectronics are marketed under the name OSTEOSTIM and include Model 2000 and earlier models S-12, HS-12 and XM-12. Zimmer, Inc. (Zimmer), a licensee of the government under the [**3] '841 patent, also markets a bone growth stimulator which the district court found to be "quite similar to the preferred embodiment of the invention shown in the patent." 658 F. Supp. at 581, 3 USPQ2d at 1571.

[*780] Normally bone fractures heal naturally as a result of the body's own reparative process.

Approximately five percent of the time, however, natural healing does not occur and bone grafting is conventionally employed to attempt to stimulate further reparative growth. 658 F. Supp. at 581-82, 3 USPQ2d at 1572.

Bone growth stimulators are particularly useful in the treatment of fractures normally requiring grafting. The success rate is at least as great as with grafting and the procedure results in less discomfort to the patient. 658 F. Supp. at 582, 3 USPQ2d at 1572. Bone growth stimulators expedite the healing of a fracture or bone defect by passing a low level constant direct current to the site of the fracture via a cathode placed internally at the site of the fracture. *Id.* The placement of the circuit-completing anode is at issue in this case.

The claim of the '841 patent at issue reads:

1. A system for [**4] expediting the healing of bone fractures and bone defects in a living being comprising:

constant current source means for providing a constant value of current despite changes in load;

means for connecting said constant current means to the living being, such connection acting to produce current flow into said fracture or defect,

said connecting means including further means for application internally of said living being at the fracture or defect site,

said constant current being a selected value within a predetermined microampere range so as to promote bone formation at the fracture or bone defect site and avoid fibrous tissue formation in other areas of the living being.

In describing the operation of the patented invention and the accused devices, the district court stated that

when using the product of either party, the cathode (negative terminal) is placed in the defect site. The Zimmer cathode is made of stainless steel, the material described in the patent. The OSTEOSTIM

cathode is made of titanium. The major difference between the products of the parties pertains to the anode (positive terminal). As disclosed in the patent drawing and accompanying [**5] description, and as marketed by Zimmer, the anode is placed on the skin of the patient. So is the power pack (current source) itself. The only internal element [in Zimmer] is the cathode -- a pin which is inserted through the skin into the defect site. This technique avoids the need for surgery; after several months of treatment, the cathode pin is simply pulled out. The OSTEOSTIM device, on the other hand, is completely implanted, an embodiment which while not shown in the patent drawing is nevertheless described. The power pack and the anode of the OSTEOSTIM are placed in soft tissue near the bone. The original OSTEOSTIM S-12 had a power pack from which two wires extended, the wires terminating respectively at a titanium cathode for placement in the defect site, and a platinum anode for placement in the soft tissue. In all of the later models, including the OSTEOSTIM-2000, the anode wire was omitted. The anode is the case itself - titanium with a patch of platinum.

658 F. Supp. at 582, 3 USPQ2d at 1572.

Because the Teletronics devices have an implanted anode, the district court stated that "the critical question in the case is whether the language [**6] of claim 1 (and with it, the dependent claims) is limited to a skin anode." 658 F. Supp. at 583, 3 USPQ at 1573. Teletronics contended before the district court that "an internal anode could not come within the literal language of claim 1 because fibrous tissue formation inevitably results from such an implant." *Id.* In finding no literal infringement, the district court held with respect to the accused device that

fibrous tissue formation could not be avoided in the dictionary sense of "keep away from" or "stay clear of".

The claim limitation directed to the avoidance of fibrous tissue means what it plainly says. Accordingly, there is no literal infringement because in the context

[*781] of the patent, even minimal fibrous tissue formation is not its avoidance. *Id.*

The district court also held that the '841 patent was not infringed under the doctrine of equivalents on the basis that the prosecution history established that the patentees, in responding to rejections by the examiner, repeatedly represented that the invention was limited to a surface or skin anode. After examining the prosecution history in detail, the district court [*7] stated: "it is clear from the file history that what convinced the Examiner to allow the claims over the prior art was the argument that a skin anode was used in the invention." 658 F. Supp. at 587, 3 USPQ2d at 1576.

On appeal, the government contends that the district court in its literal infringement analysis erred as a matter of law in its claim interpretation. According to the government, the claim limitation read as a whole requires the constant current supply to be controlled in a manner to minimize the amount of fibrous tissue formed. Teletronics counters that the district court properly interpreted the claim phrase "avoid fibrous tissue formation" and the prosecution history to find that the claim is limited to the use of a skin anode.

OPINION

I. Claim Interpretation

A. Analysis of literal infringement involves two inquiries: first the claims must be properly construed to determine their scope and then it must be determined whether the properly interpreted claims encompass the accused structure. *ZMI Corp. v. Cardiac Resuscitator Corp.*, 844 F.2d 1576, 1578, 6 USPQ2d 1557, 1559 (Fed. Cir. 1988). [*8] Claim construction is reviewed as a matter of law. However, interpretation of a claim may depend on evidentiary material about which there is a factual dispute, requiring resolution of factual issues as a basis for interpretation of the claim. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1054, 5 USPQ2d 1434, 1441 (Fed. Cir. 1988). In interpreting claims resort should be made to the claims at issue, the specification, and the prosecution history. *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 867, 228 USPQ 90, 93 (Fed. Cir. 1985). The question of literal infringement is a factual inquiry and is reviewed on a clearly erroneous standard. *Loctite Corp.*, 781 F.2d at 866, 228 USPQ at 93.

B. The district court interpreted the phrase "avoid fibrous tissue formation" [*9] as precluding the use of an implanted anode, and thus limiting the claim to a surface or skin anode. To the court, the word "avoid" based on its dictionary definition meant that there could be no fibrous tissue. Because an implanted anode inevitably resulted in some fibrous tissue, the court

determined that this placement of the anode was not covered by the claim language.

The government argues that the district court erred in its interpretation because the phrase at issue was not read in context. It contends that the claim language read as a whole only requires that there be avoidance or minimization of fibrous tissue formation by controlling or selecting the current. Thus, any fibrous tissue that may result from the implantation of the anode is immaterial.

We agree that the district court erred in its interpretation of the limitation of claim 1 and in its conclusion that such language is determinative of the anode placement. In the claim, constant current is a "selected value . . . so as to promote bone formation . . . and avoid fibrous tissue formation in other areas." Nothing in this language relates to fibrous tissue that may be formed from implantation of an anode. The plain [*10] meaning of the disputed language is only that current-related fibrous tissue formation is to be avoided.

In considering other sources for interpretation of claims, we note that the specification supports the plain meaning of the clause at issue. *See Autogiro Co. of America v. United States*, 181 Ct. Cl. 55, 384 F.2d 391, 397, 155 USPQ 697, 702-03 (1967) ("Patent law allows the inventor to be his own lexicographer. . . . the specification aids in ascertaining the scope and meaning of the language employed in the claims inasmuch as words must be used in the same way in both the claims and the [*782] specification.") The specification makes no mention of whether a skin anode or an implanted anode may cause or deter the formation of fibrous tissue. There is, however, a discussion of the increase or decrease in fibrous tissue that is formed with varying currents. Further, we find nothing in the prosecution history that would indicate that fibrous tissue resulting from implantation of an electrode was at issue or was intended to be covered by the claim language.

The claim language relied on by the district court is, therefore, not determinative of anode placement [*11] and does not require that claim 1 be limited to a surface or skin anode.

C. Claim 1 recites a "means for connecting said constant current means to the living being, such connection acting to produce current flow into said fracture or defect." Since this recitation is in the "means plus function" format permitted by 35 U.S.C. § 112, para. 6, it must be interpreted to cover the structure disclosed in the specification and the equivalents thereof. *See D.M.I., Inc. v. Deere & Co.*, 755 F.2d 1570, 1575, 225 USPQ 236, 239 (Fed. Cir. 1985).

"In construing a 'means plus function' claim, as also other types of claims, a number of factors may be

considered, including the language of the claim, the patent specification, the prosecution history of the patent, other claims in the patent, and expert testimony [citations omitted]. Once such factors are weighed, the scope of the 'means' claim may be determined." *Palumbo v. Don-Joy Co.*, 762 F.2d 969, 975, 226 USPQ 5, 8 (Fed. Cir. 1985); see also *Moeller v. Ionetics, Inc.*, 794 F.2d 653, 656, 229 USPQ 992, 994 (Fed. Cir. 1986) [**12] (resort to extrinsic evidence, such as the prosecution history, is necessary to interpret disputed claims); *SSIH Equip. S.A. v. U.S. Int'l Trade Comm'n*, 718 F.2d 365, 218 USPQ 678, 688 (Fed. Cir. 1983) (the prosecution history is always relevant to proper claim interpretation). "The prosecution history (or file wrapper) limits the interpretation of claims so as to exclude any interpretation that may have been disclaimed or disavowed during prosecution in order to obtain claim allowance." *Standard Oil Co. v. American Cyanamid Co.*, 774 F.2d 448, 452, 227 USPQ 293, 296 (Fed. Cir. 1985); see also *McGill Inc. v. John Zink Co.*, 736 F.2d 666, 673, 221 USPQ 944, 949 (Fed. Cir.), cert. denied, 469 U.S. 1037, 83 L. Ed. 2d 404, 105 S. Ct. 514 (1984).

The district court found that both implanted and surface anodes are disclosed in the specification of the '841 patent. The specification provides: "although the cathode must be placed in the fracture . . . the anode, though described as preferably being placed on the remote side [**13] of the site from the cathode, may be placed anywhere so long as it completes a circuit with the cathode." Elsewhere the specification provides that "if the anode is to be implanted, it . . . is bared of its cover." Thus, unless other relevant claim interpretation factors clearly require a different construction, the plain language of claim 1 and the specification cover an implanted anode as well as a skin or surface anode.

In its claim construction and literal infringement analysis, the district court did not consider the prosecution history but concluded for the reasons indicated in I.A., *supra*, that a surface anode was required. The prosecution history, however, was extensively discussed in the court's consideration of the doctrine of equivalents.

Prior to allowance, the applicants communicated with the examiner six times. These communications are referred to as "A" through "F" in the district court's opinion and herein. The district court concluded that because of the prosecution history appellant is "prevented from construing its claims to include an internal anode." 658 F. Supp. at 587, 3 USPQ2d at 1577. We disagree.

The district court first relied on Amendments [**14] B and C. In the former, applicants inserted the limitation "only one of said connecting means applied to the skin

surface of the living being" for the purpose of attempting to overcome a prior art rejection. This amendment was accompanied by remarks to the same effect. In Amendment C, this limitation was argued to be a distinguishing feature of the invention. [*783] Applicants' attempts to distinguish over the prior art in this fashion were unsuccessful, and the claims were later amended to remove this recitation. The arguments emphasizing the use of a skin electrode, which were made at the time the application claims explicitly contained such a limitation, cannot furnish a basis for restricting issued claim 1, which lacks any such limitation. See *Smith v. Snow*, 294 U.S. 1, 16, 79 L. Ed. 721, 55 S. Ct. 279 (1935) ("It is of no moment that in the course of the proceedings in the Patent Office the rejection of narrow claims was followed by the allowance of the broader Claim 1."); *Kistler Instrumente AG v. United States*, 224 Ct. Cl. 370, 628 F.2d 1303, 1308, 211 USPQ 920 (1980) (*aff'g* and adopting 203 USPQ 511, 516) (courts are [**15] not permitted to read "back into the claims limitations which were originally there and were removed during prosecution of the application through the Patent Office.")

In Amendment D a claim which ultimately issued as independent claim 1 was submitted for the first time. In holding claim 1 should be limited to a skin anode, the district court relied on Amendments E and F which contained arguments relative to a skin anode and which were held by the district court to be in support of the claims that finally issued. n2 From Amendment F the district court quoted the following language:

Applicants take strong exception to [the examiner's] analysis of the [Friedenberg-Kohanim article]. Nowhere in this article is there either stated or suggested that one of the electrodes need simply be applied to the surface and the other introduced into the fracture site.

These remarks were submitted to correct the examiner's characterization of a prior art reference (an article written by one of the co-inventors of the patented invention). The examiner's characterization of the reference was made in rejecting claims, at least some of which included an explicit recitation of a [**16] surface anode. Thus, these remarks are of little significance.

n2 There was some uncertainty as to which set of claims certain of these remarks applied, but the district court found that Amendments E and F related to the claims presented in Amendment D. Because we conclude that the district court

erroneously limited the claims even if the remarks in controversy did apply to the claims which issued, we need not determine whether the district court correctly resolved this dispute.

The district court also noted the following argument in Amendment F:

Applicants throughout the prosecution of this case have repeatedly attempted to convey to the Examiner the important differences between their technique where only one of the electrodes need pierce the skin *and enter the fracture site* and the other prior art arrangements where two electrodes have to pierce the skin *and then fit into prescribed locations formed in the bone structure* under study. (Emphasis added).

The quoted language does not [**17] mean that one electrode must remain on the surface of the skin. Rather, as applicants argue, it means that both of their electrodes do not have to be placed in the bone structure itself. The district court erred in construing the phrase "only one of the electrodes need pierce the skin" to mean that the other electrode must remain on the surface. This phrase, when read in conjunction with the words that follow-- "and enter the fracture site"--only serves to distinguish prior art where both electrodes were placed in the bone structure. n3 The entire emphasis of the prior art article was that the electrodes were placed in the bone for the purpose of attempting to lengthen the bone. The article was not concerned with the healing of fractures or bone defects. In the healing of fractures, it is not necessary (or desirable) to place both electrodes in the bone.

n3 The district court recognized that "there are three possible positions for placement of the anode: on the skin, in soft tissue, and in the bone. Placement within the bone must be done carefully to avoid the effect of insulation from the cortical bone." 658 F. Supp. at 583, 3 USPQ2d at 1573.

[**18]

D. "There is presumed to be a difference in meaning and scope when different words or phrases are used in separate claims. To the extent that the absence of [*784] such difference in meaning and scope would make a claim superfluous, the doctrine of claim differentiation states the presumption that the difference between claims is significant." *Tandon Corp. v. United States Int'l Trade Comm'n*, 831 F.2d 1017, 1023, 4 USPQ2d 1283, 1288

(Fed. Cir. 1987). "Where some claims are broad and others narrow, the narrow claim limitations cannot be read into the broad whether to avoid invalidity or to escape infringement." *Uniroyal, Inc.*, 837 F.2d at 1054-55, 5 USPQ2d at 1441 (quoting *D.M.I., Inc. v. Deere & Co.*, 755 F.2d at 1574, 225 USPQ at 239).

In this case the district court erroneously construed claim 1 so that its limitations are the same as dependent claim 2. Claim 2 reads in its entirety: "The system as defined in claim 1 wherein said connecting [**19] means includes means for external application to the skin surface, the internal means being a cathodic electrode, the external means being an anodic electrode." The doctrine of claim differentiation, therefore, counsels against limiting claim 1 to the use of a skin anode. See *D.M.I., Inc.*, 755 F.2d at 1574, 225 USPQ at 239.

E. On the basis of the above analysis, we conclude that the district court erred as a matter of law in its interpretation of claim 1 of the '841 patent. *Fromson v. Advance Offset Plate, Inc.*, 720 F.2d 1565, 1569, 219 USPQ 1137, 1140 (Fed. Cir. 1983).

The ordinary and accustomed meaning of claim 1 is that the current should be applied so as to avoid the formation of fibrous tissue. In support of this means plus function claim, the specification of the '841 patent disclosed both an implanted and a surface anode structure. The other claims, the specification and the prosecution history do not require a narrower construction. Thus, the district court erred in limiting claim 1 to the use of a skin anode.

II. Literal Infringement

[**20] The question of literal infringement is a factual inquiry. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d at 1054, 5 USPQ2d at 1441. Literal infringement requires that every limitation of the patent claim must be found in the accused device. *Mannesmann Demag Corp. v. Engineered Metal Prods. Co.*, 793 F.2d 1279, 1282, 230 USPQ 45, 46 (Fed. Cir. 1986). In this case, the findings of the district court establish literal infringement and, thus, there is no need to remand for a determination of the factual question of infringement under properly interpreted claims.

The district court stated in its opinion that:

The defendant's denial of infringement in this case is based solely on the defendants' anode and case being used internally. Accordingly the critical question in the case is whether the language of claim 1 (and with it the dependent claims) is limited to a skin anode.

As we have held in I., *supra*, the properly construed claims encompass both a skin anode and an implanted anode. The district court erroneously limited the claims of [**21] the '841 patent to a surface anode. Accordingly, on the position of Teletronics as stated by the district court, literal infringement is established.

The government also challenges the district court's finding of no infringement under the doctrine of equivalents. Because the accused devices literally infringe, a doctrine of equivalents inquiry is unnecessary. See *ZMI Corp. v. Cardiac Resuscitator Corp.*, 844 F.2d at 1581, 6 USPQ2d at 1562 ("When literal infringement is not found, the equitable doctrine of equivalents comes into play.").

III. Invalidity

The district court held: "if claim 1 were to be given the broad meaning which plaintiff asserts, then the patent would be invalid for a failure to comply with the specification requirements of 35 U.S.C. § 112." 658 F. Supp. at 589, 3 USPQ2d at 1577-78. According to the district court a dose response study must be performed for materials other than stainless steel to determine the optimal electrical current to be supplied and this would involve "an undue amount of experimentation. [**22]" *Id.*

In its cross-appeal Teletronics argues that the patent is invalid for non-enablement [**785] regardless of how the claims are interpreted because the disclosure does not bear a reasonable relationship to the scope of the claims.

Enablement is a legal determination which is reviewed as a matter of law. *Raytheon Co. v. Roper Co.*, 724 F.2d 951, 951-60, 220 USPQ 592, 599 (Fed. Cir. 1983). To be enabling under section 112, the patent must contain a description sufficient to enable one skilled in the art to make and use the claimed invention. *Id.* A patent may be enabling even though some experimentation is necessary; the amount of experimentation, however, must not be unduly extensive. *Atlas Powder Co. v. E.I. du Pont De Nemours & Co.*, 750 F.2d 1569, 1576, 224 USPQ 409, 413 (Fed. Cir. 1984). [**23] A patent is presumed valid, and the burden of proving invalidity, whether under section 112 or otherwise, rests with the challenger. Invalidity must be proven by facts supported by clear and convincing evidence. *Ralston Purina Co. v. Far-Mar-Co., Inc.*, 772 F.2d 1570, 1573-74, 227 USPQ 177, 178 (Fed. Cir. 1985) ("A party asserting invalidity based on 35 U.S.C. § 112 bears no less a burden . . . than any other patent

challenger.") Thus, although not mentioned by the district court, it is Teletronics' burden to show by facts supported by clear and convincing evidence that the patent was not enabling.

We note first that Teletronics admits that "the patent *does* disclose how to successfully practice the invention--if stainless steel electrodes and a current in the range of 5-20 microamperes is [sic] used." (Emphasis in original.) Lack of enablement is asserted on the basis that "the claims are not limited to the specific metal/current combination."

The district court thought that to determine the optimal electrical current for materials other [**24] than stainless steel a dose response study would be required and that this would involve an "undue amount of experimentation." The district court said "the patent does not tell a person reasonably skilled in the art how to make and use this invention because it fails to teach how to select a level of current to promote bone formation and avoid fibrous tissue . . . formation from such current" for electrodes made of materials other than stainless steel. 658 F. Supp. at 589, 3 USPQ2d at 1578. It noted that "the patent does not contain an adequate description of the methodology for a dose response study for any cathode material other than stainless steel" and that "only those who were expert in the field and actually working with bone, doing electrical stimulation experiments . . . would know how to conduct" such a study. Moreover, the district court thought that the time and expense of such a study also indicated undue experimentation would be required.

We are convinced that these findings and conclusions are insufficient to constitute clear and convincing proof of invalidity. First, it is undisputed that the patent disclosures are enabling with respect to stainless steel [**25] electrodes, with the range of current for such electrode set out in the specification. The specification shows this range of current was obtained by a dose response test. Next, according to the district court "those who were expert in the field and actually working with bone, doing electrical stimulation experiments . . . would know how to conduct a dose response study to determine the appropriate current to be used with other materials as electrodes." *Id.* The appropriate levels of current for other electrodes to promote bone growth and avoid fibrous tissue could, therefore, be determined. Finally, the emphasis by the district court on the time and cost of such studies is misplaced. While these factors may be taken into account, in the circumstances of this case we are unpersuaded that standing alone they show the experimentation to be excessive. The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent

coupled with information known in the art without undue experimentation. *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1384, 231 USPQ 81, 94 (Fed. Cir. 1986), [*26] *cert. denied*, 480 U.S. 947, 107 S. Ct. 1606, 94 L. Ed. 2d 792 (1987).

[*786] Since one embodiment is admittedly disclosed in the specification, along with the general manner in which its current range was ascertained, we are convinced that other permutations of the invention could be practiced by those skilled in the art without undue experimentation. *See SRI Int'l v. Matsushita Elec. Corp. of America*, 775 F.2d 1107, 1121, 227 USPQ 577, 586 (Fed. Cir. 1985) (the law does not require an applicant to describe in his specification every conceivable embodiment of the invention); *Hybritech Inc.*, 802 F.2d at 1384, 231 USPQ at 94 (the enablement requirement may be satisfied even though some experimentation is required). While perhaps fortuitous, as the district court found, the OSTEOSTIM device of Teletronics used a current level of 20 microamperes, within the "substantially 5 microamperes to substantially 20 microamperes" range set forth in claim 5 and disclosed in the specification.

The district court also held that if claim 1 is read to mean that the current must be applied so as to minimize fibrous tissue formation then it [*27] would be invalid under 35 U.S.C. § 112 (1982) because it would be "impossible to determine when sufficient minimization takes place to determine what current range is involved." 658 F. Supp. at 589, 3 USPQ at 1578. The district court erred as a matter of law in this holding. *Shatterproof Glass Corp. v. Libby-Owens Ford Co.*, 758 F.2d 613, 624, 225 USPQ 634, 641 (Fed. Cir.), *cert. dismissed*, 474 U.S. 976, 106 S. Ct. 340, 88 L. Ed. 2d 326 (1985). Section 112, para. 2, requires only reasonable precision in delineating the bounds of the claimed invention. *Id.* Adjusting current so as to minimize fibrous tissue formation in other parts of the living being reasonably apprises those skilled in the art of the bounds of the claimed invention and is as precise as the subject matter permits. *See id.* Thus, we hold as a matter of law that the '841 patent is enabling and that the claims satisfy 35 U.S.C. § 112, para. 2.

In its cross appeal, Teletronics argues that the specification is enabling [*28] only for the use of stainless steel while the claims are not limited in the

types of material from which the electrodes can be made. It contends that the scope of the protection must bear a reasonable relationship to the scope of enablement, citing *In re Fisher*, 57 C.C.P.A. 1099, 427 F.2d 833, 838-39, 166 USPQ 18, 23-24 (1970) ("In cases involving unpredictable factors, such as most chemical reactions and physiological activity, the scope of enablement obviously varies inversely with the degree of unpredictability of the factors involved."), and *In re Bowen*, 492 F.2d 859, 861-64, 181 USPQ 48, 50-52 (CCPA 1974) (section 112 requires that the scope of claims must bear a reasonable correlation to the scope of enablement provided by the specification to persons of ordinary skill in the art). *Fisher* and *Bowen* both involved chemical reactions, recognized by our predecessor court as having a high degree of unpredictability and therefore requiring an increased enablement disclosure. Yet, in *Bowen* the board's non-enablement rejection was reversed where the "claims literally comprehend numerous polymers in addition to the one specifically described [*29] in appellant's specification" because no persuasive reason was given by the Patent Office why the specification does not realistically enable one skilled in the art to practice the invention as broadly as it is claimed. *In re Bowen*, 492 F.2d at 863, 181 USPQ at 51-52. The same can be said here. The only impediments are the time and cost of a dose response study, which the district court found could be performed by "those who were expert in the field and actually working with bone, doing electrical stimulation experiments . . .," i.e., those skilled in the art. Moreover, as we have noted, Teletronics's device using different electrode materials actually operated within the current parameters disclosed in the specification.

We conclude that the district court erred in its nonenablement conclusion and that facts supported by clear and convincing evidence of invalidity were not adduced.

In view of our decision, we need not consider the district court's denial of attorney fees to Teletronics.

[*787] Costs

The parties shall bear their respective costs.

AFFIRMED-IN-PART AND REVERSED-IN-PART.

APPENDIX II. O.

LEXSEE 439 F.2D 220

IN RE ALFRED MARZOCCHI AND RICHARD C. HORTON

No. 8431

United States Court of Customs and Patent Appeals

58 C.C.P.A. 1069; 439 F.2d 220; 1971 CCPA LEXIS 372; 169 U.S.P.Q. (BNA)
367

Oral argument January 7, 1971

April 15, 1971

PRIOR HISTORY: [***1]

APPEAL from Patent Office, Serial No. 470,618

DISPOSITION:

Modified.

LexisNexis(R) Headnotes

COUNSEL:

Herman Hersh (McDougall, Hersh, Scott & Ladd),
attorney of record, for appellant. *Staelin & Overman*,
George A. Degnan, of counsel.

S. Wm. Cochran for the Commissioner of Patents.
Fred W. Sherling, of counsel.

OPINIONBY:

BALDWIN

OPINION: [**221]

[*1070] Before RICH, ALMOND, BALDWIN,
LANE, Associate Judges, and DURFEE, Judge, sitting
by designation

BALDWIN, Judge, delivered the opinion of the
court.

This is an appeal from the decision of the Patent
Office Board of Appeals which affirmed the final
rejection of claims 5 and 11 of appellants' application n1
under 35 USC 103 as unpatentable in view of Werner n2
and of claims 6 and 12 under 35 USC 112 as being based
on an inadequate disclosure. Claims 4 and 10 stand
allowed.

n1 Serial No. 470,618, filed July 8, 1965, for
"Fiber Coatings - Nitrogen Compounds for
Improving Adhesion of Vinyl Polymers to Glass"
as a continuation-in-part of Serial No. 96-106,
filed March 16, 1961.

n2 U.S. Patent No. 2,853,465, issued
September 23, 1958.

The Invention

The subject matter of the claims on appeal involves
a technique for improving the [***2] adhesion
characteristics between glass fibers and vinyl polymer
resins. Claim 5 is representative and reads as follows:

5. In the combination of glass fibers and a vinyl
polymer resin composition present as a coating on the
glass fiber surfaces, the improvement which comprises
mixing the vinyl polymer resin, prior to coating of the

glass fibers, with an amine compound in an amount corresponding to 2-10% by weight of the vinyl polymer resin, and in which the amine compound is monomeric vinyl pyrrolidone.

Claim 11 is drawn to the same concept as claim 5, but defines the invention as "a method of producing glass fibers coated with polyvinyl resin strongly bonded to the glass fiber surfaces." Claims 6 and 12 differ from claims 5 and 11 respectively solely in the recitation of "polyethyleneamine" as the critical "amine compound" additive.

The Section 103 Rejection

Claims 5 and 11 were rejected "as obvious in the sense of 35 USC 103 over Werner." Werner, the sole reference relied upon here, is addressed to the improvement in the bonding relationship between glass and polyvinyl halide resins. The pertinent disclosure is as follows [emphasis added]:

I have found that polyvinyl [***3] halide resins may be successfully modified so as to obtain excellent glass adhesion by employing a mixture of a polyvinyl halide and a polymer of N-vinyl pyrrolidone. By employing a mixture containing from 80 to 97% of a polyvinyl halide and from 20 to 3% of a polymer of N-vinyl pyrrolidone, which term includes homopolymers of vinyl pyrrolidone and copolymers with other polymerizable monomers, a composition is obtained having extremely high adhesion to all glass surfaces.

[*1071] On the basis of this teaching the examiner took the position, accepted by the [**222] board, that the claimed use of monomeric vinyl pyrrolidone rather than Werner's polymeric vinyl pyrrolidone would be obvious to one of ordinary skill in the art since Werner's teaching would indicate to "one skilled in the art * * * that it is the vinyl pyrrolidone moiety that is enhancing the adhesion." It was also suggested by the examiner that since the claims recite no temperature conditions for the coating operation and since monomers polymerize when heated, the claims could possibly cover circumstances wherein the monomer is polymerized during application. The board appears to have accepted this suggestion [***4] and to have extended it even further. It stated:

All of Werner's examples specify heating at elevated temperatures (110 degrees C.-130 degrees C., 165 degrees C., 325 degrees F., 350 degrees F.) with and without elevated pressures. Appellants' specification says nothing about retaining the vinyl pyrrolidone in monomeric form, much less anything about "maximizing adhesion" by preventing polymerization. Indeed, the very designation of the vinyl pyrrolidone as a "monomeric" material introduced into a polymer system for the purpose of altering the properties of such system

implies subsequent polymerization of the monomer. Appellants' further argument that the monomer has entirely different capabilities and solubilities than the polymer is also unpersuasive.

Appellants' position on appeal in response to these assertions by the examiner and board is largely to stress again the "marked difference between the properties and characteristics of a polymer as compared to a monomer," and to object to the "purely conjectural" assertion that the monomer polymerizes in the coating after it is applied. Additionally, appellants make the following contention:

Even if it were assumed that [***5] appellants' monomeric vinyl pyrrolidone is polymerized when present in the polyvinyl chloride coating, there is no teaching or suggestion in Werner that the use of monomeric vinyl pyrrolidone has any efficacy whatsoever in compositions of the type disclosed and claimed. The basis suggested by the Patent Office for the rejection is tantamount to the allegation it would be "obvious to try" the monomer. This "test" of obviousness has been frequently repudiated by this court.

The sole issue is, of course, whether the Werner teaching does suggest to a person having ordinary skill in this art that the use of monomeric vinyl pyrrolidone would have the efficacy indicated in the appealed claims. We agree with appellants that whether the monomer polymerizes is irrelevant, at least in this regard. What is relevant, however, and here determinative, is the examiner's assertion that the Werner teaching would suggest that it is the vinyl pyrrolidone moiety alone and not some other characteristic peculiar to a polymer which is efficacious in producing the desired adhesion enhancement. n3 [*1072] In the absence of anything to rebut this assertion, which is reasonable on its face, we are [***6] constrained to accept it as fact. The inferences which follow from such fact, i.e., that the monomer would possess this same characteristic and that one of ordinary skill would recognize such fact, are inescapable.

n3 Indeed, the reasonableness of such an assertion is confirmed by the very disclosure contained in appellants' application which indicates that efficacious adhesion enhancers are those "organic nitrogenous compounds which are characterized both by an organic constitution which is compatible with the vinyl polymers and by a polarity expressed in the nitrogen function." As also pointed out by appellants in their brief (about which more will be said later), the nature of the present invention resides in the use of amine compounds, broadly, as adhesion enhancers.

It is acknowledged that the above line of reasoning may be viewed as being tantamount to drawing the inference that, to one possessing the ordinary level of skill in this art, it would be "obvious [**223] to try" the monomer. Nevertheless, such an inference of fact may, at times, be enough to justify drawing the ultimate conclusion of law that the claimed subject matter as a whole would have been obvious [***7] under section 103. We are satisfied that the circumstances of this case justify an initial conclusion of obviousness. Since the record before us contains nothing to rebut that conclusion, the decision with regard to claims 5 and 11 must be affirmed.

The Section 112 Rejection

Claims 6 and 12, which recite the use of "polyethyleneamine" as the adhesion enhancer, were criticized by the examiner as being based on a disclosure which was not enabling under the first paragraph of 35 USC 112. The board affirmed his rejection of those claims with the following comment.

The term is obviously generic to a considerable number of compounds varying in the number of ethylene groups, the number of amine groups and the relationship of the polyethylene groups to the amine groups, and accordingly does not provide a reasonable guide for those seeking to improve the adherence of vinyl resins to glass.

[1] We will reverse the board's decision on this rejection since we are unable to find sufficient justification for the holding that appellants' disclosure is not enabling.

Turning specifically to the objections noted by the board as indicated above, it appears that these comments indicate [***8] nothing more than a concern over the breadth of the disputed term. If we are correct, then the relevance of this concern escapes us. It has never been contended that appellants, when they included the disputed term in their specification, intended only to indicate a single compound. Accepting, therefore, that the term is a generic one, its recitation must be taken as an assertion by appellants that all of the "considerable [*1073] number of compounds" which are included within the generic term would, as a class, be operative to produce the asserted enhancement of adhesion characteristics. The only relevant concern of the Patent Office under these circumstances should be over the truth of any such assertion. The first paragraph of § 112 requires nothing more than objective enablement. How such a teaching is set forth, either by the use of illustrative examples or by broad terminology, is of no importance.

[2] As a matter of Patent Office practice, then, a specification disclosure which contains a teaching of the manner and process of making and using the invention in terms which correspond in scope to those used in describing and defining the subject matter sought to [***9] be patented must be taken as in compliance with the enabling requirement of the first paragraph of § 112 unless there is reason to doubt the objective truth of the statements contained therein which must be relied on for enabling support. Assuming that sufficient reason for such doubt does exist, a rejection for failure to teach how to make and/or use will be proper on that basis; such a rejection can be overcome by suitable proofs indicating that the teaching contained in the specification is truly enabling.

[3] In the field of chemistry generally, there may be times when the well-known unpredictability of chemical reactions will alone be enough to create a reasonable doubt as to the accuracy of a particular broad statement put forward as enabling support for a claim. This will especially be the case where the statement is, on its face, contrary to generally accepted scientific principles. Most often, additional factors, such as the teachings in pertinent references, n4 will be available to substantiate any doubts that the asserted scope of objective enablement [**224] is in fact commensurate with the scope of protection sought and to support any demands based thereon [***10] for proof. In any event, it is incumbent upon the Patent Office, whenever a rejection on this basis is made, to explain why it doubts the truth or accuracy of any statement in a supporting disclosure and to back up assertions of its own with acceptable evidence or reasoning which is inconsistent with the contested statement. Otherwise, there would be no need for the applicant to go to the trouble and expense of supporting his presumptively accurate disclosure. Cf. *In re Gazave*, 54 CCPA 1524, 379 F.2d 973, 154 USPQ 92 (1967); *In re Chilowsky*, 43 CCPA 775, 229 F.2d 457, 108 USPQ 321 (1956).

n4 Not necessarily prior art references, it should be noted, since the question would be regarding the accuracy of a statement in the specification, not whether that statement had been made before.

In the present case, the circumstances we see do not support the reasonableness of any doubts which the Patent Office might have had [*1074] concerning the adequacy of appellants' specification disclosure to support these claims. In fact, those circumstances tend to strengthen rather than weaken appellants' claim to the breadth of protection they seek. In the first place, it has not been [***11] asserted by the Patent Office that the

58 C.C.P.A. 1069, *; 439 F.2d 220, **;
1971 CCPA LEXIS 372, ***; 169 U.S.P.Q. (BNA) 367

chemical properties of known polyethyleneamines vary to such an extent that it would not be expected by one of ordinary skill in this art that any such compound would possess the necessary capability of enhancing adhesion. Additionally, we note that polyethyleneamine is listed in appellants' specification as being only one of a much larger class of amine compounds possessing this necessary characteristic. Finally, we recognize (as did the examiner) the generic nature of appellants' broader concept, i.e., that the desired property of adhesion enhancement stems largely from the amine moiety. It does appear that variation of certain of the secondary factors mentioned by the examiner, such as molecular weight or proportion of ethylene groups, might influence to some degree or even mask the essential "amine" property of the polyethylene amine or its obviously equally essential compatibility with vinyl polymers. However, we see no basis to conclude that the ready avoidance of this result would not be within the level of

ordinary skill in this art. Compare *In re Skrivan*, 57 CCPA 1201, 427 F.2d 801, 166 USPQ 85 (1970).

Taking all these circumstances [***12] into consideration, we are constrained to conclude that the record before us contains insufficient grounds for questioning the accuracy of appellants' teaching that any polyethyleneamine (obviously excepting those whose essential "amine" characteristics and compatibility with vinyl polymers would be masked by the secondary factors mentioned) will function to accomplish the asserted result. It follows that claims 6 and 12 must be held to be supported by a disclosure which is in compliance with the requirements of the first paragraph of 35 USC 112.

Summary

The decision of the board regarding claims 5 and 11 is affirmed; that dealing with claims 6 and 12 is reversed.

APPENDIX II. P.

LEXSEE 858 F.2D 731

In re JACK R. WANDS, VINCENT R. ZURAWSKI, JR., and HUBERT J. P.
SCHOEMAKER

No. 87-1454

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

858 F.2d 731; 1988 U.S. App. LEXIS 13208; 8 U.S.P.Q.2D (BNA) 1400

September 30, 1988, Decided

SUBSEQUENT HISTORY: [**1]

As Amended October 20, 1988.

PRIOR HISTORY: Appealed from: Patent and Trademark Office, Board of Patent Appeals and Interferences.

LexisNexis(R) Headnotes

COUNSEL:

Jorge A. Goldstein, of Saidman, Sterne, Kessler & Goldstein, of Washington, District of Columbia, argued for Appellant. With him on the brief was Henry N. Wixon.

John H. Raubitschek, Associate Solicitor, Commissioner of Patents and Trademarks, of Arlington, Virginia, argued for Appellee. With him on the brief were Joseph F. Nakamura, Solicitor and Fred E. McKelvey, Deputy Solicitor.

JUDGES:

Smith, Newman, and Bissell, Circuit Judges. Newman, Circuit Judge, concurring in part, dissenting in part.

OPINIONBY:

SMITH

OPINION:

[*733] SMITH, Circuit Judge.

This appeal is from the decision of the Patent and Trademark Office (PTO) Board of Patent Appeals and Interferences (board) affirming the rejection of all remaining claims in appellant's application for a patent, serial No. 188,735, entitled "Immunoassay Utilizing Monoclonal High Affinity IgM Antibodies," which was filed September 19, 1980. n1 The rejection under 35 U.S.C. § 112, first paragraph, is based on the grounds that appellant's written specification would not enable [**2] a person skilled in the art to make the monoclonal antibodies that are needed to practice the claimed invention without undue experimentation. We reverse.

n1 *In re Wands*, Appeal No. 673-76 (Bd. Pat. App. & Int. Dec. 30, 1986).

I. Issue

The only issue on appeal is whether the board erred, as a matter of law, by sustaining the examiner's rejection for lack of enablement under 35 U.S.C. § 112, first paragraph, of all remaining claims in appellants' patent application, serial No. 188,735.

II. Background

A. The Art.

The claimed invention involves immunoassay methods for the detection of hepatitis B surface antigen by using high-affinity monoclonal antibodies of the IgM isotype. *Antibodies* are a class of proteins (immunoglobulins) that help defend the body against invaders such as viruses and bacteria. An antibody has the potential to bind tightly to another molecule, which molecule is called an *antigen*. The body has the ability to

make millions of [**3] different antibodies that bind to different antigens. However, it is only after exposure to an antigen that a complicated *immune response* leads to the production of antibodies against that antigen. For example, on the surface of hepatitis B virus particles there is a large protein called *hepatitis B surface antigen* (HBsAg). As its name implies, it is capable of serving as an antigen. During a hepatitis B infection (or when purified HBsAg is injected experimentally), the body begins to make antibodies that bind tightly and specifically to HBsAg. Such antibodies can be used as reagents for sensitive diagnostic tests (e.g., to detect hepatitis B virus in blood and other tissues, a purpose of the claimed invention). A method for detecting or measuring antigens by using antibodies as reagents is called an *immunoassay*.

Normally, many different antibodies are produced against each antigen. One reason for this diversity is that different antibodies are produced that bind to different regions (determinants) of a large antigen molecule such as HBsAg. In addition, different antibodies may be produced that bind to the same determinant. These usually differ in the tightness with [**4] which they bind to the determinant. *Affinity* is a quantitative measure of the strength of antibody-antigen binding. Usually an antibody with a higher affinity for an antigen will be more useful for immunological diagnostic tests than one with a lower affinity. Another source of heterogeneity is that there are several immunoglobulin classes or *isotypes*. Immunoglobulin G (IgG) is the most common isotype in serum. Another isotype, immunoglobulin M (IgM), is prominent early in the immune response. IgM molecules are larger than IgG molecules, and have 10 antigen-binding sites instead of the 2 that are present in IgG. Most immunoassay methods use IgG, but the claimed invention uses only IgM antibodies.

For commercial applications there are many disadvantages to using antibodies from serum. Serum contains a complex mixture of antibodies against the antigen of interest within a much larger pool of antibodies directed at other antigens. These are available only in a limited supply that ends when the donor dies. The goal of monoclonal antibody technology is to produce an unlimited supply of a single purified antibody.

The blood cells that make antibodies are *lymphocytes*. Each [**5] lymphocyte makes only one kind of antibody. During an immune response, lymphocytes exposed to [**34] their particular antigen divide and mature. Each produces a *clone* of identical daughter cells, all of which secrete the same antibody. Clones of lymphocytes, all derived from a single lymphocyte, could provide a source of a single

homogeneous antibody. However, lymphocytes do not survive for long outside of the body in cell culture.

Hybridoma technology provides a way to obtain large numbers of cells that all produce the same antibody. This method takes advantage of the properties of *myeloma* cells derived from a tumor of the immune system. The cancerous myeloma cells can divide indefinitely in vitro. They also have the potential ability to secrete antibodies. By appropriate experimental manipulations, a myeloma cell can be made to fuse with a lymphocyte to produce a single hybrid cell (hence, a hybridoma) that contains the genetic material of both cells. The hybridoma secretes the same antibody that was made by its parent lymphocyte, but acquires the capability of the myeloma cell to divide and grow indefinitely in cell culture. Antibodies produced by a clone of hybridoma [**6] cells (i.e., by hybridoma cells that are all progeny of a single cell) are called monoclonal antibodies. n2

n2 For a concise description of monoclonal antibodies and their use in immunoassay see *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1368-71, 231 USPQ 81, 82-83 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947, 107 S. Ct. 1606, 94 L. Ed. 2d 792 (1987).

B. The Claimed Invention.

The claimed invention involves methods for the immunoassay of HBsAg by using high-affinity monoclonal IgM antibodies. Jack R. Wands and Vincent R. Zurawski, Jr., two of the three coinventors of the present application, disclosed methods for producing monoclonal antibodies against HBsAg in United States patent No. 4,271,145 (the '145 patent), entitled "Process for Producing Antibodies to Hepatitis Virus and Cell Lines Therefor," which patent issued on June 2, 1981. The '145 patent is incorporated by reference into the application on appeal. The specification of the [**7] '145 patent teaches a procedure for immunizing mice against HBsAg, and the use of lymphocytes from these mice to produce hybridomas that secrete monoclonal antibodies specific for HBsAg. The '145 patent discloses that this procedure yields both IgG and IgM antibodies with high-affinity binding to HBsAg. For the stated purpose of complying with the best mode requirement of 35 U.S.C. § 112, first paragraph, a hybridoma cell line that secretes IgM antibodies against HBsAg (the 1F8 cell line) was deposited at the American Type Culture Collection, a recognized cell depository, and became available to the public when the '145 patent issued.

The application on appeal claims methods for immunoassay of HBsAg using monoclonal antibodies such as those described in the '145 patent. Most immunoassay methods have used monoclonal antibodies of the IgG isotype. IgM antibodies were disfavored in the prior art because of their sensitivity to reducing agents and their tendency to self-aggregate and precipitate. Appellants found that their monoclonal IgM antibodies could be used for immunoassay of HbsAg with unexpectedly high sensitivity and specificity. Claims 1, 3, 7, [**8] 8, 14, and 15 are drawn to methods for the immunoassay of HBsAg using high-affinity IgM monoclonal antibodies. Claims 19 and 25-27 are for chemically modified (e.g., radioactively labeled) monoclonal IgM antibodies used in the assays. The broadest method claim reads:

1. An immunoassay method utilizing an antibody to assay for a substance comprising hepatitis B-surface antigen (HBsAg) determinants which comprises the steps of:

contacting a test sample containing said substance comprising HBsAg determinants with said antibody; and

determining the presence of said substance in said sample;

wherein said antibody is a monoclonal high affinity IgM antibody having a binding affinity constant for said HBsAg determinants of at least 10^{10} M⁻¹.

Certain claims were rejected under 35 U.S.C. § 103; these rejections have not [**735] been appealed. Remaining claims 1, 3, 7, 8, 14, 15, 19, and 25-27 were rejected under 35 U.S.C. § 112, first paragraph, on the grounds that the disclosure would not enable a person skilled in the art to make and use the invention without undue experimentation. The rejection is directed solely [**9] to whether the specification enables one skilled in the art to make the monoclonal antibodies that are needed to practice the invention. The position of the PTO is that data presented by Wands show that the production of high-affinity IgM anti-HBsAg antibodies is unpredictable and unreliable, so that it would require undue experimentation for one skilled in the art to make the antibodies.

III. Analysis

A. Enablement by Deposit of Microorganisms and Cell Lines.

The first paragraph of 35 U.S.C. § 112 requires that the specification of a patent must enable a person skilled in the art to make and use the claimed invention. "Patents * * * are written to enable those skilled in the art to practice the invention." n3 A patent need not disclose what is well known in the art. n4 Although we review underlying facts found by the board under a "clearly erroneous" standard, n5 we review [**10] enablement as a question of law. n6

n3 *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1556, 220 USPQ 303, 315 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851, 105 S. Ct. 172, 83 L. Ed. 2d 107 (1984).

n4 *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463, 221 USPQ 481, 489 (Fed. Cir. 1984).

n5 *Coleman v. Dines*, 754 F.2d 353, 356, 224 USPQ 857, 859 (Fed. Cir. 1985).

n6 *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1268, 229 USPQ 805, 810 (Fed. Cir. 1986), *cert. denied*, 479 U.S. 1030, 107 S. Ct. 875, 93 L. Ed. 2d 829 (1987); *Raytheon Co. v. Roper Corp.*, 724 F.2d 951, 960 n.6, 220 USPQ 592, 599 n.6 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 835, 83 L. Ed. 2d 69, 105 S. Ct. 127 (1984).

Where an invention depends on the use of living materials such as microorganisms or cultured cells, it may be impossible [**11] to enable the public to make the invention (i.e., to obtain these living materials) solely by means of a written disclosure. One means that has been developed for complying with the enablement requirement is to deposit the living materials in cell depositories which will distribute samples to the public who wish to practice the invention after the patent issues. n7 Administrative guidelines and judicial decisions have clarified the conditions under which a deposit of organisms can satisfy the requirements of section 112. n8 A deposit has been held necessary for enablement where the starting materials (i.e., the living cells used to practice the invention, or cells from which the required cells can be produced) are not readily available to the public. n9 Even when starting materials are available, a deposit has been necessary where it would require undue experimentation to make the cells of the invention from the starting materials. n10

N7 *In re Argoudelis*, 58 C.C.P.A. 769, 434 F.2d 1390, 1392-93, 168 USPQ 99, 101-02 (CCPA 1970).

858 F.2d 731, *, 1988 U.S. App. LEXIS 13208, **;
8 U.S.P.Q.2D (BNA) 1400

n8 *In re Lundak*, 773 F.2d 1216, 227 USPQ 90 (Fed. Cir. 1985); *Feldman v. Aunstrup*, 517 F.2d 1351, 186 USPQ 108 (CCPA 1975), *cert. denied*, 424 U.S. 912, 47 L. Ed. 2d 316, 96 S. Ct. 1109 (1976); Manual of Patent Examining Procedure (MPEP) 608.01(p)(C) (5th ed. 1983, rev. 1987). *See generally* Hampar, *Patenting of Recombinant DNA Technology: The Deposit Requirement*, 67 J. Pat. Trademark Off. Soc'y 569 (1985). [**12]

n9 *In re Jackson*, 217 USPQ 804, 807-08 (Bd. App. 1982) (strains of a newly discovered species of bacteria isolated from nature); *Feldman*, 517 F.2d 1351, 186 USPQ 108 (uncommon fungus isolated from nature); *In re Argoudelis*, 434 F.2d at 1392, 168 USPQ at 102 (novel strain of antibiotic-producing microorganism isolated from nature); *In re Kropp*, 143 USPQ 148, 152 (Bd. App. 1959) (newly discovered microorganism isolated from soil).

n10 *In re Forman*, 230 USPQ 546, 547 (Bd. Pat. App. & Int. 1986) (genetically engineered bacteria where the specification provided insufficient information about the amount of time and effort required); *In re Lundak*, 773 F.2d 1216, 227 USPQ 90 (unique cell line produced from another cell line by mutagenesis).

In addition to satisfying the enablement requirement, deposit of organisms also can be used to establish the filing date of the application as the prima facie date of invention, n11 [*736] and to satisfy the requirement under 35 U.S.C. § 114 [**13] that the PTO be guaranteed access to the invention during pendency of the application. n12 Although a deposit may serve these purposes, we recognized, in *In re Lundak*, n13 that these purposes, nevertheless, may be met in ways other than by making a deposit.

n11 *In re Lundak*, 773 F.2d at 1222, 227 USPQ at 95-96; *In re Feldman*, 517 F.2d at 1355, 186 USPQ at 113; *In re Argoudelis*, 434 F.2d at 1394-96, 168 USPQ at 103-04 (Baldwin, J. concurring).

n12 *In re Lundak*, 773 F.2d at 1222, 227 USPQ at 95-96; *In re Feldman*, 517 F.2d at 1354, 186 USPQ at 112.

n13 *In re Lundak*, 773 F.2d at 1222, 227 USPQ at 95-96.

A deposit also may satisfy the best mode requirement of section 112, first paragraph, and it is for this reason that the 1F8 hybridoma was deposited in connection with the '145 patent and the current application. Wands does not challenge the statements by the examiner to the effect that, [**14] although the deposited 1F8 line enables the public to perform immunoassays with antibodies produced by that single hybridoma, the deposit does not enable the generic claims that are on appeal. The examiner rejected the claims on the grounds that the written disclosure was not enabling and that the deposit was inadequate. Since we hold that the written disclosure fully enables the claimed invention, we need not reach the question of the adequacy of deposits.

B. Undue Experimentation.

Although inventions involving microorganisms or other living cells often can be enabled by a deposit, n14 a deposit is not always necessary to satisfy the enablement requirement. n15 No deposit is necessary if the biological organisms can be obtained from readily available sources or derived from readily available starting materials through routine screening that does not require undue experimentation. n16 Whether the specification in an application involving living cells (here, hybridomas) is enabled without [**15] a deposit must be decided on the facts of the particular case. n17

n14 *In re Argoudelis*, 434 F.2d at 1393, 168 USPQ at 102.

n15 *Tabuchi v. Nubel*, 559 F.2d 1183, 194 USPQ 521 (CCPA 1977).

n16 *Id.* at 1186-87, 194 USPQ at 525; *Merck & Co. v. Chase Chem. Co.*, 273 F. Supp. 68, 77, 155 USPQ 139, 146 (D.N.J. 1967); *Guaranty Trust Co. v. Union Solvents Corp.*, 54 F.2d 400, 403-06, 12 U.S.P.Q. (BNA) 47, 50-53 (D. Del. 1931), *aff'd*, 61 F.2d 1041, 15 U.S.P.Q. (BNA) 237 (3d Cir. 1932), *cert. denied*, 288 U.S. 614, 77 L. Ed. 987, 53 S. Ct. 405 (1933); MPEP 608.01(p)(C) ("No problem exists when the microorganisms used are known and readily available to the public.").

n17 *In re Jackson*, 217 USPQ at 807; *see In re Metcalfe*, 56 C.C.P.A. 1191, 410 F.2d 1378, 1382, 161 USPQ 789, 792 (CCPA 1969).

Appellants contend that their written specification fully [**16] enables the practice of their claimed invention because the monoclonal antibodies needed to perform the immunoassays can be made from readily available starting materials using methods that are well known in the monoclonal antibody art. Wands states that application of these methods to make high-affinity IgM anti-HBsAg antibodies requires only routine screening, and that does not amount to undue experimentation. There is no challenge to their contention that the starting materials (i.e., mice, HBsAg antigen, and myeloma cells) are available to the public. The PTO concedes that the methods used to prepare hybridomas and to screen them for high-affinity IgM antibodies against HBsAg were either well known in the monoclonal antibody art or adequately disclosed in the '145 patent and in the current application. This is consistent with this court's recognition with respect to another patent application that methods for obtaining and screening monoclonal antibodies were well known in 1980. n18 The sole issue is whether, in this particular case, it would require undue experimentation to produce high-affinity IgM monoclonal antibodies.

n18 *Hybritech*, 802 F.2d at 1384, 231 USPQ at 94.

[**17]

Enablement is not precluded by the necessity for some experimentation such as [**737] routine screening. n19 However, experimentation needed to practice the invention must not be undue experimentation. n20 "The key word is 'undue,' not 'experimentation.'" n21

The determination of what constitutes undue experimentation in a given case requires the application of a standard of reasonableness, having due regard for the nature of the invention and the state of the art. *Ansul Co. v. Uniroyal, Inc.* [448 F.2d 872, 878-79; 169 USPQ 759, 762-63 (2d Cir. 1971), *cert. denied*, 404 U.S. 1018, 30 L. Ed. 2d 666, 92 S. Ct. 680 (1972)]. The test is not merely quantitative, since a considerable amount of experimentation is permissible, if it is merely routine, or if the specification in question provides a reasonable amount of guidance with respect to the direction in which the experimentation should proceed * * *. n22

n19 *Id.*; *Atlas Powder Co. v. E.I. DuPont De Nemours & Co.*, 750 F.2d 1569, 1576, 224 USPQ 409, 413 (Fed. Cir. 1984); *In re Angstadt*, 537 F.2d at 502-504, 190 USPQ at 218; *In re Geerdes*, 491 F.2d 1260, 1265, 180 USPQ 789, 793 (CCPA 1974); *Minerals Separation, Ltd. v. Hyde*, 242 U.S. 261, 270-71, 61 L. Ed. 286, 37 S. Ct. 82 (1916). [**18]

n20 *Hybritech*, 802 F.2d at 1384, 231 USPQ at 94; *W.L. Gore*, 721 F.2d at 1557, 220 USPQ at 316; *In re Colianni*, 561 F.2d 220, 224, 195 USPQ 150, 153 (CCPA 1977) (Miller, J., concurring).

n21 *In re Angstadt*, 537 F.2d at 504, 190 USPQ at 219.

n22 *In re Jackson*, 217 USPQ at 807.

The term "undue experimentation" does not appear in the statute, but it is well established that enablement requires that the specification teach those in the art to make and use the invention without undue experimentation. n23 Whether undue experimentation is needed is not a single, simple factual determination, but rather is a conclusion reached by weighing many factual considerations. The board concluded that undue experimentation would be needed to practice the invention on the basis of experimental data presented by Wands. These data are not in dispute. However, Wands and the board disagree strongly on the conclusion that [**19] should be drawn from that data.

n23 *See Hybritech*, 802 F.2d at 1384, 231 USPQ at 94; *Atlas Powder*, 750 F.2d at 1576, 224 USPQ at 413.

Factors to be considered in determining whether a disclosure would require undue experimentation have been summarized by the board in *In re Forman*. n24 They include (1) the quantity of experimentation necessary, (2) the amount of direction or guidance presented, (3) the presence or absence of working examples, (4) the nature of the invention, (5) the state of the prior art, (6) the relative skill of those in the art, (7) the predictability or unpredictability of the art, and (8) the breadth of the claims. n25

n24 *In re Forman*, 230 USPQ at 547.

n25 *Id.*; see *In re Colianni*, 561 F.2d at 224, 195 USPQ at 153 (Miller, J., concurring); *In re Rainer*, 52 C.C.P.A. 1593, 347 F.2d 574, 577, 146 USPQ 218, 221 (CCPA 1965).

[**20]

In order to understand whether the rejection was proper, it is necessary to discuss further the methods for making specific monoclonal antibodies. The first step for making monoclonal antibodies is to immunize an animal. The '145 patent provides a detailed description of procedures for immunizing a specific strain of mice against HBsAg. Next the spleen, an organ rich in lymphocytes, is removed and the lymphocytes are separated from the other spleen cells. The lymphocytes are mixed with myeloma cells, and the mixture is treated to cause a few of the cells to fuse with each other. Hybridoma cells that secrete the desired antibodies then must be isolated from the enormous number of other cells in the mixture. This is done through a series of screening procedures.

The first step is to separate the hybridoma cells from unfused lymphocytes and myeloma cells. The cells are cultured in a medium in which all the lymphocytes and myeloma cells die, and only the hybridoma cells survive. The next step is to isolate and clone hybridomas that make antibodies [*738] that bind to the antigen of interest. Single hybridoma cells are placed in separate chambers and are allowed to grow and divide. [**21] After there are enough cells in the clone to produce sufficient quantities of antibody to analyze, the antibody is assayed to determine whether it binds to the antigen. Generally, antibodies from many clones do not bind the antigen, and these clones are discarded. However, by screening enough clones (often hundreds at a time), hybridomas may be found that secrete antibodies against the antigen of interest.

Wands used a commercially available radioimmunoassay kit to screen clones for cells that produce antibodies directed against HBsAg. In this assay the amount of radioactivity bound gives some indication of the strength of the antibody-antigen binding, but does not yield a numerical affinity constant, which must be measured using the more laborious Scatchard analysis. In order to determine which anti-HBsAg antibodies satisfy all of the limitations of appellants' claims, the antibodies require further screening to select those which have an IgM isotype and have a binding affinity constant of at least $10^{<9>} M^{<-1>}$. n26 The PTO does not question that the screening techniques used by Wands were well known in the monoclonal antibody art.

n26 The examiner, the board, and Wands all point out that, technically, the strength of antibody-HBsAg binding is measured as *avidity*, which takes into account multiple determinants on the HBsAg molecule, rather than affinity. Nevertheless, despite this correction, all parties then continued to use the term "affinity." We will use the terminology of the parties. Following the usage of the parties, we will also use the term "high-affinity" as essentially synonymous with "having a binding affinity constant of at least $10^{<9>} M^{<-1>}$."

[**22]

During prosecution Wands submitted a declaration under 37 C.F.R. § 1.132 providing information about all of the hybridomas that appellants had produced before filing the patent application. The first four fusions were unsuccessful and produced no hybridomas. The next six fusion experiments all produced hybridomas that made antibodies specific for HBsAg. Antibodies that bound at least 10,000 cpm in the commercial radioimmunoassay were classified as "high binders." Using this criterion, 143 high-binding hybridomas were obtained. In the declaration, Wands stated that n27

It is generally accepted in the art that, among those antibodies which are binders with 50,000 cpm or higher, there is a very high likelihood that high affinity (K_a [greater than] $10^{<9>} M^{<-1>}$) antibodies will be found. However, high affinity antibodies can also be found among high binders of between 10,000 and 50,000, as is clearly demonstrated in the Table.

The PTO has not challenged this statement.

n27 A table in the declaration presented the binding data for antibodies from every cell line. Values ranged from 13,867 to 125,204 cpm, and a substantial proportion of the antibodies showed binding greater than 50,000 cpm. In confirmation of Dr. Wands' statement, two antibodies with binding less than 25,000 cpm were found to have affinity constants greater than $10^{<9>} M^{<-1>}$.

[**23]

The declaration stated that a few of the high-binding monoclonal antibodies from two fusions were chosen for further screening. The remainder of the antibodies and the hybridomas that produced them were saved by freezing. Only nine antibodies were subjected to further

analysis. Four (three from one fusion and one from another fusion) fell within the claims, that is, were IgM antibodies and had a binding affinity constant of at least $10^{9.5}$ M⁻¹. Of the remaining five antibodies, three were found to be IgG, while the other two were IgM for which the affinity constants were not measured (although both showed binding well above 50,000 cpm).

Apparently none of the frozen cell lines received any further analysis. The declaration explains that after useful high-affinity IgM monoclonal antibodies to HBsAg had been found, it was considered unnecessary to return to the stored antibodies to screen for more IgMs. Wands says that the existence of the stored hybridomas was disclosed to the PTO to comply with the requirement under 37 C.F.R. § 1.56 that applicants fully disclose all of their relevant [*739] data, and not just favorable results. n28 How these stored hybridomas are viewed [**24] is central to the positions of the parties.

n28 See *Rohm & Haas Co. v. Crystal Chem. Co.*, 722 F.2d 1556, 220 USPQ 289 (Fed. Cir. 1983).

The position of the board emphasizes the fact that since the stored cell lines were not completely tested, there is no proof that any of them are IgM antibodies with a binding affinity constant of at least $10^{9.5}$ M⁻¹. Thus, only 4 out of 143 hybridomas, or 2.8 percent, were proved to fall within the claims. Furthermore, antibodies that were proved to be high-affinity IgM came from only 2 of 10 fusion experiments. These statistics are viewed by the board as evidence that appellants' methods were not predictable or reproducible. The board concludes that Wands' low rate of demonstrated success shows that a person skilled in the art would have to engage in undue experimentation in order to make antibodies that fall within the claims.

Wands views the data quite differently. Only nine hybridomas were actually analyzed beyond the initial screening for HBsAg [**25] binding. Of these, four produced antibodies that fell within the claims, a respectable 44 percent rate of success. (Furthermore, since the two additional IgM antibodies for which the affinity constants were never measured showed binding in excess of 50,000 cpm, it is likely that these also fall within the claims.) Wands argues that the remaining 134 unanalyzed, stored cell lines should not be written off as failures. Instead, if anything, they represent partial success. Each of the stored hybridomas had been shown to produce a high-binding antibody specific for HBsAg. Many of these antibodies showed binding above 50,000 cpm and are thus highly likely to have a binding affinity constant of at least $10^{9.5}$ M⁻¹. Extrapolating from

the nine hybridomas that were screened for isotype (and from what is well known in the monoclonal antibody art about isotype frequency), it is reasonable to assume that the stored cells include some that produce IgM. Thus, if the 134 incompletely analyzed cell lines are considered at all, they provide some support (albeit without rigorous proof) to the view that hybridomas falling within the claims are not so rare that undue experimentation would be needed [**26] to make them.

The first four fusion attempts were failures, while high-binding antibodies were produced in the next six fusions. Appellants contend that the initial failures occurred because they had not yet learned to fuse cells successfully. Once they became skilled in the art, they invariably obtained numerous hybridomas that made high-binding antibodies against HBsAg and, in each fusion where they determined isotype and binding affinity they obtained hybridomas that fell within the claims.

Wands also submitted a second declaration under 37 C.F.R. § 1.132 stating that after the patent application was submitted they performed an eleventh fusion experiment and obtained another hybridoma that made a high-affinity IgM anti-HBsAg antibody. No information was provided about the number of clones screened in that experiment. The board determined that, because there was no indication as to the number of hybridomas screened, this declaration had very little value. While we agree that it would have been preferable if Wands had included this information, the declaration does show that when appellants repeated their procedures they again obtained a hybridoma that produced an antibody that [**27] fit all of the limitations of their claims.

We conclude that the board's interpretation of the data is erroneous. It is strained and unduly harsh to classify the stored cell lines (each of which was proved to make high-binding antibodies against HBsAg) as failures demonstrating that Wands' methods are unpredictable or unreliable. n29 At worst, they prove nothing at all about the probability of success, and merely show [*740] that appellants were prudent in not discarding cells that might someday prove useful. At best, they show that high-binding antibodies, the starting materials for IgM screening and Scatchard analysis, can be produced in large numbers. The PTO's position leads to the absurd conclusion that the more hybridomas an applicant makes and saves without testing, the less predictable the applicant's results become. Furthermore, Wands' explanation that the first four attempts at cell fusion failed only because they had not yet learned to perform fusions properly is reasonable in view of the fact that the next six fusions were all successful. The record indicates that cell fusion is a technique that is well known to those of ordinary skill in the monoclonal

antibody [**28] art, and there has been no claim that the fusion step should be more difficult or unreliable where the antigen is HBsAg than it would be for other antigens.

n29 Even if we were to accept the PTO's 2.8% success rate, we would not be required to reach a conclusion of undue experimentation. Such a determination must be made in view of the circumstances of each case and cannot be made solely by reference to a particular numerical cutoff.

When Wands' data is interpreted in a reasonable manner, analysis considering the factors enumerated in *In re Forman* leads to the conclusion that undue experimentation would not be required to practice the invention. Wands' disclosure provides considerable direction and guidance on how to practice their invention and presents working examples. There was a high level of skill in the art at the time when the application was filed, and all of the methods needed to practice the invention were well known.

The nature of monoclonal antibody technology is that it involves screening [**29] hybridomas to determine which ones secrete antibody with desired characteristics. Practitioners of this art are prepared to screen negative hybridomas in order to find one that makes the desired antibody. No evidence was presented by either party on how many hybridomas would be viewed by those in the art as requiring undue experimentation to screen. However, it seems unlikely that undue experimentation would be defined in terms of the number of hybridomas that were never screened. Furthermore, in the monoclonal antibody art it appears that an "experiment" is not simply the screening of a single hybridoma, but is rather the entire attempt to make a monoclonal antibody against a particular antigen. This process entails immunizing animals, fusing lymphocytes from the immunized animals with myeloma cells to make hybridomas, cloning the hybridomas, and screening the antibodies produced by the hybridomas for the desired characteristics. Wands carried out this entire procedure three times, and was successful each time in making at least one antibody that satisfied all of the claim limitations. Reasonably interpreted, Wands' record indicates that, in the production of high-affinity IgM antibodies [**30] against HBsAg, the amount of effort needed to obtain such antibodies is not excessive. Wands' evidence thus effectively rebuts the examiner's challenge to the enablement of their disclosure. n30

n30 *In re Strahilevitz*, 668 F.2d 1229, 1232, 212 USPQ 561, 563 (CCPA 1982).

IV. Conclusion

Considering all of the factors, we conclude that it would not require undue experimentation to obtain antibodies needed to practice the claimed invention. Accordingly, the rejection of Wands' claims for lack of enablement under 35 U.S.C. § 112, first paragraph, is reversed.

REVERSED

CONCURBY:

NEWMAN (In Part)

DISSENTBY:

NEWMAN (In Part)

DISSENT:

NEWMAN, Circuit Judge, concurring in part, dissenting in part.

A

I concur in the court's holding that additional samples of hybridoma cell lines that produce these high-affinity IgM monoclonal antibodies need not be deposited. This invention, as described by Wands, is not a selection of a few rare cells from many possible cells. To the contrary, [**31] Wands states that all monoclonally produced IgM antibodies to hepatitis B surface antigen have the desired high avidity and other favorable properties, and that all are readily preparable by now-standard techniques.

Wands states that his United States Patent No. 4,271,145 describes fully operable techniques, and is distinguished from his [*741] first four failed experiments that are referred to in the Rule 132 affidavit. Wands argues that these biotechnological mechanisms are relatively well understood and that the preparations can be routinely duplicated by those of skill in this art, as in *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1380, 231 USPQ 81, 94 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947, 107 S. Ct. 1606, 94 L. Ed. 2d 792 (1987). I agree that it is not necessary that there be a deposit of multiple exemplars of a cell system that is readily reproduced by known, specifically identified techniques.

B

I would affirm the board's holding that Wands has not complied with 35 U.S.C. § 112, first paragraph, in that he has not provided data sufficient to support the breadth of his generic [**32] claims. Wands' claims on appeal include the following:

19. Monoclonal high affinity IgM antibodies immunoreactive with HBsAg determinants, wherein said antibodies are coupled to an insoluble solid phase, and wherein the binding affinity constant of said antibodies for said HBsAg determinants is at least $10^{9.5}$ M⁻¹.

26. Monoclonal high affinity IgM antibodies immunoreactive with HBsAg determinants wherein said antibodies are detectably labelled.

Wands states that he obtained 143 "high binding monoclonal antibodies of the right specificity" in the successful fusions; although he does not state how they were determined to be high binding or of the right specificity, for Wands also states that only nine of these 143 were tested.

Of these nine, four (three from one fusion and one from another fusion) were found to have the claimed high affinity and to be of the IgM isotype. Wands states that the other five were either of a different isotype or their affinities were not determined. (This latter statement also appears to contradict his statement that all 143 were "high binding".)

Wands argues that a "success rate of four out of nine", or 44.4%, is sufficient to [**33] support claims to the entire class. The Commissioner deems the success rate to be four out of 143, or 2.8%; to which Wands responds with statistical analysis as to how unlikely it is that Wands selected the only four out of 143 that worked. Wands did not, however, prove the right point. The question is whether Wands, by testing nine out of 143 (the Commissioner points out that the randomness of the sample was not established), and finding that four out of the nine had the desired properties, has provided sufficient experimental support for the breadth of the requested claims, in the context that "experiments in genetic engineering produce, at best, unpredictable results", quoting from *Ex parte Forman*, 230 USPQ 546, 547 (Bd. Pat. App. and Int. 1986).

The premise of the patent system is that an inventor, having taught the world something it didn't know, is encouraged to make the product available for public and commercial benefit, by governmental grant of the right to exclude others from practice of that which the inventor

has disclosed. The boundary defining the excludable subject matter must be carefully set: it must protect the inventor, so that commercial development [**34] is encouraged; but the claims must be commensurate with the inventor's contribution. Thus the specification and claims must meet the requirements of 35 U.S.C. § 112. *In re Fisher*, 57 C.C.P.A. 1099, 427 F.2d 833, 839, 166 USPQ 18, 23-24 (CCPA 1970).

As the science of biotechnology matures the need for special accommodation, such as the deposit of cell lines or microorganisms, may diminish; but there remains the body of law and practice on the need for sufficient disclosure, including experimental data when appropriate, that reasonably support the scope of the requested claims. That law relates to the sufficiency of the description of the claimed invention, and if not satisfied by deposit, must independently meet the requirements of Section 112.

Wands is not claiming a particular, specified IgM antibody. He is claiming all such monoclonal antibodies in assay for hepatitis B surface antigen, based on his teaching that such antibodies have uniformly reproducible high avidity, free of the known [*742] disadvantages of IgM antibodies such as tendency to precipitate or aggregate. It is incumbent upon Wands to provide reasonable support for [**35] the proposed breadth of his claims. I agree with the Commissioner that four exemplars shown to have the desired properties, out of the 143, do not provide adequate support.

Wands argues that the law should not be "harsher" where routine experiments take a long time. However, what Wands is requesting is that the law be less harsh. As illustrated in extensive precedent on the question of how much experimentation is "undue", each case must be determined on its own facts. *See, e.g., W.L. Gore & Assocs., Inc. v. Garlock, Inc.* 721 F.2d 1540, 1557, 220 USPQ 303, 316 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851, 105 S. Ct. 172, 83 L. Ed. 2d 107 (1984); *In re Angstadt*, 537 F.2d 498, 504, 190 USPQ 214, 218 (CCPA 1976); *In re Cook*, 58 C.C.P.A. 1049, 439 F.2d 730, 734-35, 169 USPQ 298, 302-03 (CCPA 1971).

The various criteria to be considered in determining whether undue experimentation is required are discussed in, for example, *Fields v. Conover*, 58 C.C.P.A. 1366, 443 F.2d 1386, 170 USPQ 276 (CCPA 1971); *In re Rainer*, 52 C.C.P.A. 1593, 347 F.2d 574, 146 USPQ 218 (CCPA 1965); *Ex parte Forman*, 230 USPQ at 547. [**36] Wands must provide sufficient data or authority to show that his results are reasonably predictable within the scope of the claimed generic invention, based on experiment and/or scientific theory. In my view he has not met this burden.

APPENDIX II. Q.

LEXSEE 30 F.3D 1475

IN RE DAVID C. PAULSEN

94-1012

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

30 F.3d 1475; 1994 U.S. App. LEXIS 19882; 31 U.S.P.Q.2D (BNA) 1671

August 3, 1994, Decided

PRIOR HISTORY: [**1] Appealed from: United States Patent and Trademark Office Board of Patent Appeals and Interferences. (Reexamination Nos. 90/002,014, 90/002,053, and 90/002,179)

DISPOSITION: AFFIRMED.

LexisNexis(R) Headnotes

COUNSEL: J. Georg Seka, Attorney, Townsend and Townsend Khourie and Crew, of San Francisco, California, argued for appellant.

Harris Pitlick, Attorney, Commissioner of Patents and Trademarks, of Arlington, Virginia, argued for appellee. With him on the brief was Fred E. McKelvey.

JUDGES: Before NIES, MICHEL, and LOURIE, Circuit Judges.

OPINIONBY: LOURIE

OPINION: [*1477] LOURIE, Circuit Judge.

AST Research, Inc., (AST) n1 appeals from the July 23, 1993 decision of the United States Patent and Trademark Office (PTO) Board of Patent Appeals and Interferences sustaining the final rejection upon reexamination of claims 1-4, 6, 9-12, and 18-34 of U.S. Patent 4,571,456. We affirm.

n1 AST Research is the current record owner of the patent in issue.

[*1478] BACKGROUND

The '456 patent, entitled "Portable Computer," was issued to David C. Paulsen et al., on February 18, 1986. The claims of the patent are directed [**2] to a portable computer contained within a compact metal case. n2 A salient feature of the claimed invention is its "clam shell" configuration, in which the computer's display housing is connected to the computer at its midsection by a hinge assembly that enables the display to swing from a closed, latched position for portability and protection to an open, erect position for viewing and operation. Computers consistent with this design are commonly referred to as "laptop" computers.

n2 Claim 1 is the broadest claim in the '456 patent and is illustrative of the claimed invention. The claim reads as follows:

1. A portable computer constructed to be contained within an outer case for transport and to be erectable to a viewing and operating configuration for use, said computer comprising

a base,
a display housing,
a top cover,
a rear cover,

hinge means for permitting swinging movement of the display housing about an axis of rotation adjacent the rear end of the display housing and from a closed and latched position of the display housing on the base to an erected

position for viewing by an operator, and including stop means for holding the display housing at the desired angle for viewing,

the hinge means being located in a mid portion of the base and wherein the hinge means permit swinging movement of the display housing to an erected position in which the inner surface of the display housing is held in an upward and rearwardly inclined angle for viewing by an operator in front of the computer, and

including a keyboard in the portion of the base which is exposed by the movement of the display housing to the erected position.

[**3]

On April 27, 1990, and subsequently on June 12, 1990 and October 22, 1990, requests were filed in the PTO for reexamination of the '456 patent. See 35 U.S.C. § 302 (1988). The requests were consolidated into a single proceeding for the reexamination of claims 1 through 34. n3 On August 9, 1991, the examiner issued a final office action in the reexamination rejecting claims 1-4, 6, 7, 9-12, and 18-34. Independent claims 1 and 18 were rejected under 35 U.S.C. § 102(b) (1988) as being anticipated by Japanese Application 47-14961 to Yokoyama. Additionally, claims 1-4, 6, 7, 9-12, and 18-34 were rejected under 35 U.S.C. § 103 (1988) as being obvious over the Yokoyama reference in view of other prior art. n4

n3 As originally issued, the '456 patent contained claims 1 through 19. New claims 20 through 34 were subsequently added during reexamination.

n4 Claims 5, 8, and 13-17 were allowed by the examiner in the reexamination proceeding. These claims are not at issue in this appeal.

[**4]

On appeal, the Board affirmed the examiner's rejections except as to claim 7. In sustaining the rejections of claims 1 and 18, the Board rejected the appellant's n5 contention that Yokoyama is not a proper prior art reference under sections 102 or 103. The Board concluded that although Yokoyama discloses a calculator, a calculator is a type of computer. The Board also rejected the appellant's argument that Yokoyama is a non-enabling reference. Respecting the § 103 rejection of claims 2-4, 6, 9-12, and 19-34, the Board adopted the examiner's determination that the cited prior art would

have suggested the claim subject matter to a person of ordinary skill in the art. n6

n5 The party in interest during the reexamination proceeding was Grid Systems Corp., the original assignee of the '456 patent.

n6 Because the Board adopted the examiner's position as its own, we shall refer to the examiner's findings and conclusions as those of the Board.

AST, the present assignee of the '456 patent, now appeals from the Board's [**5] decision.

DISCUSSION

Claims 1 and 18

We first address AST's challenge to the Board's determination that claims 1 and 18 are anticipated by the Yokoyama reference. Anticipation is a question of fact subject to review under the "clearly erroneous" standard. *In re King*, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986). A rejection for anticipation under section 102 requires that each and every limitation of the claimed invention be disclosed in a single [*1479] prior art reference. *In re Spada*, 911 F.2d 705, 708, 15 USPQ2d 1655, 1657 (Fed. Cir. 1990). In addition, the reference must be enabling and describe the applicant's claimed invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention. *Id.*

The Yokoyama reference discloses a desktop calculator contained within a housing having the form of a portable attache case. The front half of the case consists of a lid that is hinged at the midsection of the case. Connected to the inside of the lid is a display which is able to be viewed when the lid is opened to a vertical position. A keyboard [**6] is also exposed for operation when the lid is opened. When the device is to be transported, the lid is closed and latched to protect the display and the keyboard. Notwithstanding that Yokoyama discloses a device meeting the express limitations set out in claims 1 and 18 relating to a base, a display housing, a keyboard, etc., AST maintains that the claims are not anticipated by Yokoyama because that reference discloses a calculator, not a computer. n7 AST contends that the Board erred in construing the term "computer" broadly to encompass a calculator such as that disclosed in Yokoyama.

n7 AST does not dispute that all the limitations of claims 1 and 18 are otherwise described in the Yokoyama reference.

We note at the outset that the term "computer" is found only in the preamble of the claims at issue. The preamble of a claim does not limit the scope of the claim when it merely states a purpose or intended use of the invention. See *DeGeorge v. Bernier*, 768 F.2d 1318, 1322 n.3, 226 USPQ 758, 761 n.3 (Fed. Cir. 1985). [**7] However, terms appearing in a preamble may be deemed limitations of a claim when they "give meaning to the claim and properly define the invention." *Gerber Garment Technology, Inc. v. Lectra Sys., Inc.*, 916 F.2d 683, 688, 16 USPQ2d 1436, 1441 (Fed. Cir. 1990) (quoting *Perkin-Elmer Corp. v. Computervision Corp.*, 732 F.2d 888, 896, 221 USPQ 669, 675 (Fed. Cir.), cert. denied, 469 U.S. 857, 83 L. Ed. 2d 120, 105 S. Ct. 187 (1984)). Although no "litmus test" exists as to what effect should be accorded to words contained in a preamble, review of a patent in its entirety should be made to determine whether the inventors intended such language to represent an additional structural limitation or mere introductory language. *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257, 9 USPQ2d 1962, 1966 (Fed. Cir. 1989); *In re Stencel*, 828 F.2d 751, 754, 4 USPQ2d 1071, 1073 (Fed. Cir. 1987).

In the instant case, review of the '456 patent [**8] as a whole reveals that the term "computer" is one that "breathes life and meaning into the claims and, hence, is a necessary limitation to them." *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 866, 228 USPQ 90, 92 (Fed. Cir. 1984). Thus, to anticipate claims 1 and 18, the Yokoyama reference must disclose a type of "computer." See *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 678, 7 USPQ2d 1315, 1317 (Fed. Cir. 1988) (prior art reference must contain preamble limitations). However, to properly compare Yokoyama with the claims at issue, we must construe the term "computer" to ascertain its scope and meaning. Claim construction is a legal question that we address de novo. See *Carroll Touch, Inc. v. Electro Mechanical Sys., Inc.*, 15 F.3d 1573, 1577, 27 USPQ2d 1836, 1839 (Fed. Cir. 1993).

Pursuant to its practice of giving claims in a reexamination their broadest reasonable interpretation consistent with the specification, see *In re Etter*, 756 F.2d 852, 858, 225 USPQ 1, 5 (Fed. Cir. 1985), the [**9] Board construed the term "computer" to include a calculator. The Board's interpretation was supported by authoritative lexicographic sources that confirmed that a calculator is considered to be a particular type of computer by those of ordinary skill in the art. AST alleges that the Board's interpretation was erroneous because it ignores the inventors' own definition of

"computer." AST asserts that the specification plainly indicates that the inventors intended to limit the claimed invention to a device having a display with graphics and text capability, sufficient data processing capacity, communication ports, a telephone connection, [*1480] etc., features normally absent in a calculator.

In an effort to avoid the anticipating disclosure of Yokoyama, AST engages in a post hoc attempt to redefine the claimed invention by impermissibly incorporating language appearing in the specification into the claims. Although "it is entirely proper to use the specification to interpret what the patentee meant by a word or phrase in the claim, . . . this is not to be confused with adding an extraneous limitation appearing in the specification, which is improper. By 'extraneous,' we mean a limitation [**10] read into a claim from the specification wholly apart from any need to interpret . . . particular words or phrases in the claim." *E.I. Du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433, 7 USPQ2d 1129, 1131 (Fed. Cir.), cert. denied, 488 U.S. 986, 102 L. Ed. 2d 572, 109 S. Ct. 542 (1988). Moreover, when interpreting a claim, words of the claim are generally given their ordinary and accustomed meaning, unless it appears from the specification or the file history that they were used differently by the inventor. See *Carroll Touch*, 15 F.3d at 1577, 27 USPQ2d at 1840.

The term "computer" is not associated with any one fixed or rigid meaning, as confirmed by the fact that it is subject to numerous definitions and is used to describe a variety of devices with varying degrees of sophistication and complexity. However, despite the lack of any standard definition for this ubiquitous term, it is commonly understood by those skilled in the art that "at the most fundamental level, a device is a computer if it is capable of [**11] carrying out calculations." *National Advanced Sys., Inc. v. United States*, 26 F.3d 1107, slip op. at 10 (Fed. Cir. 1994). AST cannot dispute that a calculator falls within that basic definition. That a calculator may be a "limited function" computer as opposed to a "full function" computer does not change the fact that it is nonetheless a computer. n8

n8 We are unpersuaded by the declarations submitted by the appellants which draw a distinction between a calculator and a computer based on comparative functions and capabilities. As the Board correctly concluded, such extrinsic evidence fails to rebut the premise that a calculator is a computer, albeit one with limited functions.

Although an inventor is indeed free to define the specific terms used to describe his or her invention, this must be done with reasonable clarity, deliberateness, and precision. "Where an inventor chooses to be his own lexicographer and to give terms uncommon meanings, he must set out his uncommon definition in some manner within [**12] the patent disclosure" so as to give one of ordinary skill in the art notice of the change. See *Intellicall, Inc., v. Phonometrics, Inc.*, 952 F.2d 1384, 1387-88, 21 USPQ2d 1383, 1386 (Fed. Cir. 1992). Here, the specification of the '456 patent does not clearly redefine the term "computer" such that one of ordinary skill in the art would deem it to be different from its common meaning. The specification merely describes in a general fashion certain features and capabilities desirable in a portable computer. This description, however, is far from establishing a specialized definition restricting the claimed invention to a computer having a specific set of characteristics and capabilities.

We conclude that the Board did not clearly err in determining that the Yokoyama reference meets all the limitations of claims 1 and 18 as properly construed, including the "computer" limitation.

Alternatively, AST asserts that Yokoyama does not anticipate claims 1 and 18 because it is not enabling. AST argues that Yokoyama only discloses a box for a calculator and thus does not teach how to make and use a portable calculator. This argument, however, fails [**13] to recognize that a prior art reference must be "considered together with the knowledge of one of ordinary skill in the pertinent art." *In re Samour*, 571 F.2d 559, 562, 197 USPQ 1, 3-4 (CCPA 1978); see also *DeGeorge*, 768 F.2d at 1323, 226 USPQ at 762 (Fed. Cir. 1985) (a reference "need not, however, explain every detail since [it] is speaking to those skilled in the art"). As the Board found below, the level of skill to which Yokoyama is addressed was "quite advanced" at the time the '456 patent was filed and that "one of ordinary skill in the art [**1481] certainly was capable of providing the circuitry necessary to make the device operable for use as a computer." We discern no clear error in the Board's findings and conclude as a matter of law that Yokoyama is sufficiently enabling to serve as a section 102(b) reference. n9 See *Gould v. Quigg*, 822 F.2d 1074, 1077, 3 USPQ2d 1302, 1303-04 (Fed. Cir. 1987) (ultimate issue of enablement is one of law based on underlying factual findings).

n9 We also note that under the enablement standard that AST would have us apply to Yokoyama, the '456 patent itself would be non-enabling. The '456 patent similarly relies on the knowledge and skill of those skilled in the art. If

detailed disclosure regarding implementation of known electronic and mechanical components necessary to build a computer were essential for an anticipating reference, then the disclosure in the '456 patent would also fail to satisfy the enablement requirement. See *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1569, 7 USPQ2d 1057, 1063 (Fed. Cir. 1988).

[**14]

Accordingly, we affirm the Board's rejection of claims 1 and 18 as being anticipated by Yokoyama. As a result, we need not review the obviousness rejections of these claims. See *In re Baxter Travenol Labs*, 952 F.2d 388, 391, 21 USPQ2d 1281, 1285 (Fed. Cir. 1992) ("Since anticipation is the ultimate of obviousness, the subject matter of these claims is necessarily obvious and we need not consider them further."). Additionally, because AST does not argue the patentability of claims 9-12 and 19-27 separately from that of claims 1 and 18, the appeal of these claims also fails. See *In re Albrecht*, 579 F.2d 92, 93-94, 198 USPQ 208, 209 (CCPA 1978); *In re King*, 801 F.2d at 1325, 231 USPQ at 137.

Claims 2-4, 6, and 28-34

Next, AST challenges the Board's rejection of claims 2-4, 6, and 28-34 on the ground of obviousness. Obviousness is a question of law to be determined from the facts. *In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Thus, the Board's conclusion of obviousness is reviewed [**15] for error as a matter of law, *In re De Blauwe*, 736 F.2d 699, 703, 222 USPQ 191, 195 (Fed. Cir. 1984), and underlying factual inquiries are reviewed for clear error, *In re Caveney*, 761 F.2d 671, 674, 226 USPQ 1, 3 (Fed. Cir. 1985).

1. Non-Analogous Art

AST argues that claims 2, 6, and 28-34, which add particular features to the hinge and latch means of the display housing, n10 were erroneously rejected over non-analogous references directed to hinges and latches as used in a desktop telephone directory, a piano lid, a kitchen cabinet, a washing machine cabinet, a wooden furniture cabinet, or a two-part housing for storing audio cassettes. AST maintains that because the references pertain to fields of endeavor entirely unrelated to computers and are not pertinent to the problems faced by the present inventors, they do not render the claims obvious. It argues that the cited references, dealing with such articles as cabinets and washing machines, do not deal with the particular environment presented in portable computers. This argument rests on too narrow a

view of what prior art is pertinent [**16] to the invention here.

n10 Generally, claims 2 and 6, both depending from claim 1, recite torsion spring means and recessed latch means for the display housing, respectively. Claims 28, 29, 30, 33, and 34 are directed to a portable computer having concealed hinges, and claims 31 and 32 recite recessed latch means and retractable legs, respectively.

Whether a prior art reference is "analogous" is a fact question that we review under the "clearly erroneous" standard. In re Clay, 966 F.2d 656, 658, 23 USPQ2d 1058, 1060 (Fed. Cir. 1992). Although there is little dispute that the prior art references cited here (other than Yokoyama) are not within the same field of endeavor as computers, such references may still be analogous if they are "reasonably pertinent to the particular problem with which the inventor is involved." Id.; see also Heidelberg Druckmaschinen AG v. Hantscho Commercial Prods., Inc., 21 F.3d 1068, 1072, 30 USPQ2d 1377, 1379 (Fed. Cir. 1994). [**17] The problems encountered by the inventors of the '456 patent were problems that were not unique to portable computers. They concerned how to connect and secure the computer's display housing to the computer while meeting certain size constraints [*1482] and functional requirements. The prior art cited by the examiner discloses various means of connecting a cover (or lid) to a device so that the cover is free to swing radially along the connection axis, as well as means of securing the cover in an open or closed position. We agree with the Board that given the nature of the problems confronted by the inventors, one of ordinary skill in the art "would have consulted the mechanical arts for housings, hinges, latches, springs, etc." Thus, the cited references are "reasonably pertinent" and we therefore conclude that the Board's finding that the references are analogous was not clearly erroneous.

2. Secondary Considerations

In support of its contention that the Board erred in rejecting claims 2-4, 6, and 28-34 as obvious, AST points to evidence of commercial success, copying, and professional recognition of Grid laptop computers, devices covered by claims 1 and 18 of the '456 patent. For example, [**18] from the introduction of their laptop computers in 1983 to the end of 1990, Grid enjoyed cumulative sales of approximately \$ 489 million in addition to licensing royalties of \$ 7.5 million. Grid

also received several design awards and exceptional praise from the industry press.

Although such evidence is indeed impressive, AST has not shown that it is relevant to the claims at issue and thus entitled to weight. When a patentee offers objective evidence of nonobviousness, there must be a sufficient relationship between that evidence and the patented invention. See *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392, 7 USPQ2d 1222, 1226 (Fed. Cir.), cert. denied, 488 U.S. 956, 102 L. Ed. 2d 383, 109 S. Ct. 395 (1988). "The term 'nexus' is used, in this context, to designate a legally and factually sufficient connection between the proven success and the patented invention, such that the objective evidence should be considered in the determination of nonobviousness. The burden of proof as to this connection or nexus resides with the patentee." Id. Here, AST [**19] has failed to carry its burden.

AST limits its argument respecting the evidence adduced to demonstrate nonobviousness to laptop computers covered by claims 1 and 18, claims which we have previously concluded are unpatentable under section 102. n11 AST has not established that the commercial success, copying, and professional recognition experienced by Grid laptop computers are probative of the nonobviousness of the inventions of claims 2-4, 6, and 28-34. It has not been shown that such evidence is relevant to a computer within the scope of these claims, i.e., that it is attributable to the inventions of these claims, rather than to extraneous factors such as advertising and marketing or to the features possessed by the computers of claims 1 and 18. Because AST has failed to establish a sufficient legal relationship between the purported evidence of nonobviousness and the claimed invention, evidence pertinent to claims 1 and 18 therefore carries no weight with respect to claims 2-4, 6, and 28-34.

n11 The only evidence connecting the purported commercial success and professional praise with the '456 patent is the declaration of J. Georg Seka, counsel for AST, stating that claims 1 and 18 cover the Grid "Compass" laptop computer and certain models made by Toshiba. Even assuming that a nexus exists as to those two claims, evidence of nonobviousness is irrelevant for patentability purposes when an invention is anticipated under section 102.

[**20]

3. Obviousness Generally

30 F.3d 1475, *, 1994 U.S. App. LEXIS 19882, **;
31 U.S.P.Q.2D (BNA) 1671

Beyond what we have said respecting the applicability of the cited prior art and the asserted evidence of secondary considerations, we have considered AST's basic contention that the prior art does not suggest the invention of the rejected claims and view it to be unpersuasive. In reviewing the Board's obviousness conclusions, we have been guided by the well-settled principles that the claimed invention must be considered as a whole, multiple cited prior art references must suggest the desirability of being combined, and the references must be viewed without the benefit of hindsight afforded by the disclosure. See *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir.), cert. denied, 479 U.S. 827, 107 S. Ct. 106, 93 [*1483] L. Ed. 2d 55 (1986).

We have carefully reviewed the prior art of record and conclude that the Board did not err in rejecting claims 2-4, 6, and 28-34 as having been obvious.

CONCLUSION

The Board did not clearly err in rejecting claims 1 and 18 as being anticipated by the Yokoyama reference. Consequently, [**21] the rejection of claims 9-12 and 19-27 must also be affirmed. The Board did not err in rejecting claims 2-4, 6, and 28-34 as being obvious over Yokoyama and other prior art. Accordingly, we affirm the decision of the Board.

AFFIRMED

APPENDIX II. R.

LEXSEE 133 F.3D 1473

**MULTIFORM DESICCANTS, INC., Plaintiff-Cross Appellant, v. MEDZAM, LTD
Defendant-Appellant.**

96-1255, 96-1274

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

133 F.3d 1473; 1998 U.S. App. LEXIS 697; 45 U.S.P.Q.2D (BNA) 1429

January 15, 1998, Decided

PRIOR HISTORY: [**1] Appealed from: United States District Court for the Western District of New York. Judge Elfvin.

DISPOSITION: AFFIRMED.

LexisNexis(R) Headnotes

COUNSEL: Michael R. McGee, McGee & Gelman, of Buffalo, New York, argued for plaintiff-cross appellant.

Jeremiah J. McCarthy, Phillips, Lytle, Hitchcock, Blaine & Huber, of Buffalo, New York, argued for defendant-appellant.

JUDGES: Before NEWMAN, CLEVINGER, and SCHALL, Circuit Judges.

OPINIONBY: NEWMAN

OPINION: [*1475] NEWMAN, Circuit Judge.

In this patent suit, the United States District Court for the Western District of New York n1 held that United States Patent No. 4,853,266, entitled "Liquid Absorbing and Immobilizing Packet Containing a Material for Treating the Absorbed Liquid" (the '266 patent), owned by Multiform Desiccants, Inc., was not infringed by the similar product sold by Medzam, Ltd. The district court entered judgment in favor of Medzam, did not decide the issue of patent validity, and denied Medzam's request for attorney fees. Multiform appeals the judgment of non-infringement, and Medzam appeals the denial of attorney fees and the decision not to reach the issue of validity.

n1 Multiform Desiccants, Inc. v. Medzam, Ltd., 1995 U.S. Dist. LEXIS 18548, No. 91-CV-0095E(H), 1995 WL 737929 (W.D.N.Y. Dec. 7, 1995).

[**2]

THE TECHNOLOGY

The invention described and claimed in the '266 patent is a packet for use in controlling spilled liquids. In typical use the packet is placed in an outer shipping container that encloses an inner container holding a hazardous liquid such as medical waste or body fluids. Should the inner container break or leak, the released liquid encounters the packet in the outer container. The packet envelope, which is made of a soluble material, disintegrates and releases materials that absorb, immobilize, and treat the spilled liquid. The absorbing and immobilizing material is preferably sodium polyacrylate, a known absorbent that expands and gels on contact with liquid. The treating material may be a known disinfectant, scent, deodorizer, etc., depending on the intended use of the packet.

Medzam's accused packet, called the Red-Z Safety Pac, is designed and sold for the same uses as the Multiform packet. The Medzam envelope is made of porous material such as is used for tea bags, and contains the [*1476] known absorbing and immobilizing material potassium polyacrylate and a disinfectant. When spilled liquid penetrates the porous envelope, the polyacrylate inside the envelope starts [**3] to absorb and expand. The expanding absorbent splits open the envelope, releasing its contents for further absorption.

LITERAL INFRINGEMENT

Patent infringement occurs when a device (or composition or method), that is literally covered by the claims or is equivalent to the claimed subject matter, is made, used, or sold, without the authorization of the patent holder, during the term of the patent. See 35 U.S.C. § 271. The claims are concise statements of the subject matter for which the statutory right to exclude is secured by the grant of the patent. Since a full and complete understanding of the scope of the claims is requisite to determining whether the patent is infringed, technical terms or words of art or special usages in the claims, if in dispute, are construed or clarified by the court before the construed claims are applied to the accused device. On appellate review the Federal Circuit again construes the claims, determining de novo the correct construction. See *Markman v. Westview Instruments*, 52 F.3d 967, 979-81, 34 U.S.P.Q.2D (BNA) 1321, 1329-31 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370, 116 S. Ct. 1384, 38 U.S.P.Q.2D (BNA) 1461, 134 L. Ed. 2d 577 (1996). [**4]

On occasion the issue of literal infringement may be resolved with the step of claim construction, for upon correct claim construction it may be apparent whether the accused device is within the claims. See, e.g., *Strattec Security Corp. v. Gen. Automotive Specialty*, 126 F.3d 1411, 1419, 44 U.S.P.Q.2D (BNA) 1030, 1036 (Fed. Cir. 1997); *Applied Materials, Inc. v. Advanced Semiconductor Materials America, Inc.*, 98 F.3d 1563, 1572, 40 U.S.P.Q.2D (BNA) 1481, 1488 (Fed. Cir. 1996). The district court so viewed this case. Although the cause was fully tried to a jury, after trial the judge dismissed the jury without requesting a verdict, citing the Federal Circuit's decision in *Markman* and stating that "This question is one of claim construction, a question of law."

Claims 1 and 6

In the '266 patent the packet is claimed as a combination of the degradable envelope, the absorbing material, and the treating material. A second group of claims describes the envelope in terms of its function, in the form authorized by 35 U.S.C. § 112 P6; these claims are discussed post. Claims 1 and 6 are representative of the first group of claims:

1. A packet for absorbing and immobilizing a [**5] liquid comprising an envelope which is degradable in said liquid, a first material in said envelope for absorbing and immobilizing said liquid, and a second material confined in said envelope for additionally treating said liquid which is absorbed and immobilized to nullify a specific undesirable quality thereof.

6. In an outer container having an inner container with liquid from which said liquid can leak, an absorbent packet located between said inner and outer containers for absorbing and immobilizing said liquid within said outer container in the event of leakage of said liquid from said inner container comprising an envelope which is degradable in said liquid, a first material in said envelope for absorbing and immobilizing said liquid, and a second material confined in said envelope for additionally treating said liquid which is absorbed and immobilized to nullify a specific undesirable quality thereof.

(Emphases added.) Medzam conceded that its packet contains all of the elements of claims 1 and 6 except the "degradable" envelope. Medzam argued that its envelope is not degradable, when that term is correctly construed, and thus that the claims are not infringed. [**6]

The disputed issue is the meaning of the term "degradable" in characterizing the claimed envelope. The district court defined this term with an eye to the accused envelope. The court held that the terms "degrade" and "degradable," as used in the '266 patent, mean that the envelope at least partially dissolves and thereby disintegrates in the liquid. The court held that this meaning of "degradable" does not include the mode of operation of the Medzam packet, wherein the envelope bursts open by expansion of the contents but the envelope itself does not dissolve and disintegrate by direct action of the liquid.

[*1477] Multiform states that this claim construction is incorrect, and that upon correct construction a finding of infringement is inevitable. Multiform argues that "degradable" must first be construed based on the '266 patent documents, without reference to the accused device, see *Jurgens v. McKasy*, 927 F.2d 1552, 1560, 18 U.S.P.Q.2D (BNA) 1031, 1037 (Fed. Cir. 1991) ("claim is construed without regard to the accused product"); *Scripps Clinic & Research Found. v. Genentech, Inc.*, 927 F.2d 1565, 1580, 18 U.S.P.Q.2D (BNA) 1001, 1013 (Fed. Cir. 1991) (the words of the claims are independently construed, [**7] focussing on the disputed elements), and that as used in the '266 patent "degradable" is not limited to dissolution and disintegration, but means any loss in the containment function of the envelope. Multiform cites dictionaries showing this broader meaning, and states that a person of ordinary skill would construe "degradable," as applied to these envelopes, as meaning a loss in their containment function.

It is the person of ordinary skill in the field of the invention through whose eyes the claims are construed. Such person is deemed to read the words used in the patent documents with an understanding of their meaning in the field, and to have knowledge of any special meaning and usage in the field. The inventor's words that are used to describe the invention -- the inventor's lexicography -- must be understood and interpreted by the court as they would be understood and interpreted by a person in that field of technology. Thus the court starts the decisionmaking process by reviewing the same resources as would that person, viz., the patent specification and the prosecution history. These documents have legal as well as technological content, for they show not only the framework [**8] of the invention as viewed by the inventor, but also the issues of patentability as viewed by the patent examiner.

During patent prosecution Multiform submitted dictionary definitions of "degradable" from Webster's New Collegiate Dictionary (1976), explaining the submission as follows:

The word "degrade" includes the definitions of "to deprive of standing or true function" and "to impair in respect of some physical property." Thus when the envelope is dry and not degraded, its true function is to contain its contents. However, once it is exposed to liquid, it is deprived of its standing or true function and it has its physical property of containing its contents impaired.

Multiform states that this definition is comprehensive of the degradation of the Medzam envelope that bursts apart and thus loses its true function, and is not limited to an envelope that degrades by dissolving. Multiform states that it is not necessary for the packet to disintegrate in order to degrade. Medzam responds that Multiform offered these definitions only after Multiform became aware of the Medzam packet, and that the definitions are at odds with the plain reading of the specification. [**9]

Multiform argues that, in keeping with the rule that an inventor may be his own lexicographer, its definition of "degradable" must prevail. When the meaning of a term is sufficiently clear in the patent specification, that meaning shall apply. See *Intellicall, Inc. v. Phonometrics, Inc.*, 952 F.2d 1384, 1388, 21 U.S.P.Q.2D (BNA) 1383, 1387 (Fed. Cir. 1992); *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 889, 221 U.S.P.Q. (BNA) 1025, 1031 (Fed. Cir. 1988). This rule of construction recognizes that the inventor may have imparted a special meaning to a term in order to convey a character or property or nuance relevant to the particular invention. Such special meaning, however, must be sufficiently

clear in the specification that any departure from common usage would be so understood by a person of experience in the field of the invention.

Thus we review, de novo, the meaning of "degradable" in claims 1 and 6. We start with the specification. See *Slimfold Mfg. Co. v. Kinkead Industries, Inc.*, 810 F.2d 1113, 1116, 1 U.S.P.Q.2D (BNA) 1563, 1566 (Fed. Cir. 1987) ("Claims are not interpreted in a vacuum, but are part of and are read in light of the specification.") The '266 specification describes [**10] the Multiform envelope as made of soluble starch, such that "when the aqueous solution comes into contact with the envelope, it degrades it . . ." '266 patent, col. 1, lines 21-23. The specification explains that degradation of the envelope results from dissolution of the soluble envelope material. The specification illustrates an envelope [*1478] whose inner layer contains a dot matrix pattern of insoluble material that permits heat-sealing, and in discussing this pattern the specification explains that it is the soluble portion that results in degradation of the envelope: "The dot matrix pattern, or any other suitable discontinuous pattern, permits liquid, which may not otherwise be able to dissolve the material of coating 17, to completely degrade envelope 11 because there are uncoated spaces 18 between the dots of the coating 17 through which liquid can pass." '266 patent, col. 3, lines 5-10. The district court discussed the specification in reaching its conclusion, and also reviewed the prosecution history. The court referred to United States Patent No. 4,124,116 to McCabe, which describes a water-soluble envelope that releases its contents upon contact with spilled aqueous liquid. [**11] The McCabe envelope is made of two sheets, one of which is made of soluble starch. The district court observed that "Multiform distinguished this invention to the PTO, not by asserting a distinction between degrade and dissolve, but by noting that the '266 Patent included a second material for treating the absorbed liquid." 1995 WL 737929 at *11. We agree that this analysis is correct.

The district court concluded that the specification and the prosecution history do not support a meaning of "degradable" that would include an envelope that bursts open from inner pressure without any dissolution. The district court defined "degradable" in light of the mode of action of the accused device, a pragmatic expedient relevant to the issue in litigation. Thus the court held that Multiform's dictionary definitions added during patent prosecution, although stating a broad definition of "degradable," could not serve to enlarge the scope of the claims in order to cover the Medzam device. The district court did not accept Multiform's position that the dictionary definitions provided during the prosecution

simply clarified the inventor's original usage of "degradable." We agree with this analysis. [**12]

Courts must exercise caution lest dictionary definitions, usually the least controversial source of extrinsic evidence, be converted into technical terms of art having legal, not linguistic, significance. The best source for understanding a technical term is the specification from which it arose, informed, as needed, by the prosecution history. The evolution of restrictions in the claims, in the course of examination in the PTO, reveals how those closest to the patenting process -- the inventor and the patent examiner -- viewed the subject matter. See *Hoechst Celanese Corp. v. BP Chemicals Ltd.*, 78 F.3d 1575, 1578, 38 U.S.P.Q.2D (BNA) 1126, 1129 (Fed. Cir. 1996) ("A technical term used in a patent document is interpreted as having the meaning that it would be given by persons experienced in the field of the invention, unless it is apparent from the patent and the prosecution history that the inventor used the term with a different meaning.") When the specification explains and defines a term used in the claims, without ambiguity or incompleteness, there is no need to search further for the meaning of the term.

We conclude that the meaning of "degradable" in claims 1 and 6 (and the claims [**13] dependent thereon) is limited to the dissolution/degradation of the envelope as described in the specification. The court correctly excluded the meaning whereby the envelope "degrades" by bursting instead of dissolving, and correctly held that "degradable" means that there must be at least partial dissolution of the envelope. Upon this claim interpretation, the district court concluded that there could not be literal infringement of claims 1 and 6. We agree, for this claim interpretation eliminated the Medzam envelope, which bursts but does not dissolve, from the literal meaning and scope of the claims.

Claims 11 to 15

During pendency of the '266 application claims 11-18 were added to describe the envelope in terms of its function, in accordance with the form authorized by 35 U.S.C. § 112 P6. n2 Claims 11-15, asserted against the Medzam packet, do not contain the word "degradable." Claim 11 is representative:

N2 § 112 P6. An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

[**14]

[*1479] 11. A packet for absorbing and immobilizing a liquid comprising a first material which will absorb and immobilize said liquid, a second material for additionally treating said liquid which is absorbed and immobilized to nullify a specific undesirable quality of said liquid, and means for containing said first and second materials while said means are dry and for releasing said first and second materials on contact of said means with said liquid to thereby permit said first and second materials to absorb and immobilize and treat said liquid.

(Emphasis added.) In adding these "means-for" claims Multiform's attorney wrote to the patent examiner that the word "degradable" was ambiguous in that it could be interpreted "as synonymous with 'disintegrate,' which is not necessary for the packet to function properly." The attorney submitted the dictionary definitions that we discussed in connection with claims 1 and 6. Multiform argues that the grant of claims 11-15 makes clear that neither the applicant nor the examiner viewed the invention as limited to a dissolving, disintegrating envelope.

A claim containing a functional limitation written in means-for form is literally infringed [**15] when the accused device performs the function stated in the claim, by means of structure, material, or acts described in the specification or equivalents thereof. See *Texas Instruments Corp. v. United States Int'l Trade Comm'n*, 805 F.2d 1558, 1562, 231 U.S.P.Q. (BNA) 833, 834-35 (Fed. Cir. 1986) (equivalency of structure, materials, or acts with respect to the claimed function is a matter of literal infringement). Thus § 112 P6 facilitates the mechanics of claiming, by permitting the use of functional terms in claims while incorporating, from the specification, the breadth as well as the details of how the function is performed. However, claims written in the means-for form of § 112 P6 do not, by virtue of this form, acquire a scope as to the function beyond that which is supported in the specification, or as to the structure beyond equivalents of that shown in the specification.

In determining whether there is literal infringement under § 112 P6, the first step in interpretation of the claim is determination of the meaning of the words used to describe the claimed function, if such meaning is in dispute. This claim interpretation is deemed to be a matter of law, and is reviewed de [**16] novo on appeal. *Markman*, 52 F.3d at 979-81, 34 U.S.P.Q.2D (BNA) at 1329-31. Medzam conceded that all of the elements of claim 11 are present in its device, except for the element now claimed in terms of its function of

containing and releasing the absorbing and treating materials.

The district court found that the function of containing and releasing the contents of the packet does not embrace all envelopes whose contents are released on contact with liquid. The court stressed the description of the envelope in the '266 specification as made of "degradable starch paper," "degradable in water and other liquids," "able to dissolve," and "practically entirely disintegrated," in finding that the function of releasing the envelope contents must be performed by an envelope that disintegrates by dissolution. The court then found that since the Medzam envelope does not dissolve, it does not perform the function required by claims 11-15.

Multiform argues that the function of containing and releasing the contents of the envelope is plainly performed by the Medzam envelope, and that even if the Medzam envelope's structure and material are not the same as described in the '266 specification, they [**17] are equivalent means of performing the same function. The district court found that the structure and material of Medzam's porous envelope, which works by penetration of the liquid through the envelope fabric, are not equivalent to the starch paper described in the '266 specification, which dissolves and disintegrates. The district court's finding of non-infringement is reviewed for clear error. *Biodex Corp. v. Loredan Biomedical, Inc.*, 946 F.2d 850, 852, 20 U.S.P.Q.2D (BNA) 1252, 1254 (Fed. Cir. 1991); *Durango Associates, Inc. v. Reflange, Inc.*, 843 F.2d 1349, 1357, 6 U.S.P.Q.2D (BNA) 1290, 1295 (Fed. Cir. 1988).

Multiform invokes the doctrine of claim differentiation, which presumes that there is a difference in scope among the claims of a patent. *Tandon Corp. v. United States Int'l Trade Comm'n*, 831 F.2d 1017, 1023, 4 U.S.P.Q.2D (BNA) 1283, 1288 (Fed. Cir. 1987); [**1480] *Autogiro Co. of America v. United States*, 181 Ct. Cl. 55, 384 F.2d 391, 404, 155 U.S.P.Q. (BNA) 697, 708 (Ct. Cl. 1967). Multiform states that this doctrine requires that claims 11-15 be viewed separately from claims 1 and 6, and that a broader interpretation is warranted because claims 11-15 are not limited to a degradable envelope, but are [**18] directed primarily to the function of containing and releasing the contents. However, the doctrine of claim differentiation can not broaden claims beyond their correct scope, determined in light of the specification and the prosecution history and any relevant extrinsic evidence. As explained in *Tandon*, 831 F.2d at 1023, 4 U.S.P.Q.2D (BNA) at 1288, claims that are written in different words may ultimately cover substantially the same subject matter. See also *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1269, 229 U.S.P.Q. (BNA) 805, 810 (Fed. Cir. 1986)

(affirming district court's construction of a claim although it rendered a dependent claim redundant). We affirm the district court's ruling that the functions stated in claims 11-15, as performed by the structure and materials shown in the '266 specification and equivalents thereof, are not literally met in the Medzam envelope.

DOCTRINE OF EQUIVALENTS

Multiform argues that even on the district court's interpretation of the claims, the Medzam packet infringes under the doctrine of equivalents. The doctrine of equivalents, of common law origin, serves to prevent a "fraud on the patent." *Graver Tank & Mfg. Co. v. Linde Air Products Co.*, [**19] 339 U.S. 605, 607, 85 U.S.P.Q. (BNA) 328, 330, 94 L. Ed. 1097, 70 S. Ct. 854 (1950). Thus the doctrine of equivalents balances the purpose of fairness to inventors lest the patent be unjustly circumvented, against the purpose of patent claims to state clear boundaries of the patent grant, in fair notice of its scope. *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 137 L. Ed. 2d 146, 117 S. Ct. 1040, 1051, 41 U.S.P.Q.2D (BNA) 1865, 1873 (1997).

Applying *Graver Tank* and *Warner-Jenkinson*, we review whether the Medzam porous envelope performs substantially the same function as that of the dissolving envelope of the '266 patent and, if so, whether it is performed in substantially the same way to achieve substantially the same result. *Graver Tank*, 339 U.S. at 608, 85 U.S.P.Q. (BNA) at 330. We also apply the requirement that all of the claim elements or functions must be present in the accused device, literally or by an equivalent element or function. *Warner-Jenkinson*, 117 S. Ct. at 1054, 41 U.S.P.Q.2D (BNA) at 1875.

Determination of infringement under the doctrine of equivalents occurs after the claims have been construed as a matter of law. The trier of fact, applying the claims as construed, finds whether [**20] the accused device, element by element, is equivalent to that which has been patented. The court also determines whether there is any estoppel derived from the prosecution history that bars remedy even when there is technologic equivalency, for the patentee is precluded from reaching, under the doctrine of equivalents, subject matter that was disclaimed in order to obtain the patent.

The district court found that the Medzam envelope performs the function of releasing its contents in a substantially different way than does the envelope of the '266 patent, in that the Medzam envelope is not soluble in and does not degrade in the liquid. Although Multiform argues that the Medzam packet functions in a way that is "consistent" with the '266 invention, for the Medzam porous envelope releases its contents upon contact with liquid, the district court found a porous envelope that bursts with inner pressure to be

substantially different from a degradable envelope that dissolves. This finding has not been shown to be clearly erroneous.

Multiform argues that the interchangeability of the envelopes weighs heavily on the side of equivalency. Interchangeability is a significant factor in determination [**21] of equivalency. In *Warner-Jenkinson*, 117 S. Ct. at 1052-53, 41 U.S.P.Q.2D (BNA) at 1874, the Court explained that interchangeability need not be known at the time the patent application was filed, and that substitution of a later-developed element does not insulate the combination from a finding of equivalency. See *Atlas Powder Co. v. E.I. Du Pont De Nemours & Co.*, 750 F.2d 1569, 1581, 224 U.S.P.Q. (BNA) 409, 417 (Fed. Cir. 1984) [*1481] (separately patentable element did not avoid equivalency). However, the district court found that "the Red-Z Zafety Pac envelope would not be known as interchangeable with a degradable envelope by one reasonably skilled in the art." 1995 WL 737929 at *13. The modes of dissolving and bursting are not clearly interchangeable, and we do not discern clear error in the district court's finding that they were not interchangeable.

The district court's finding of non-infringement under the doctrine of equivalents is not clearly erroneous, and must be affirmed.

VALIDITY

After the trial Medzam withdrew its antitrust, unfair competition, unfair trade practice, and tort-based counterclaims; no counterclaims remained. Although Medzam continued to assert patent invalidity as an [**22] affirmative defense to infringement, the district court stated, upon finding non-infringement, that it "need not reach the issue of whether Medzam has overcome the presumption of validity regarding the '266 Patent." 1995 WL 737929 at *14. The district court recognized that it could, in its discretion, decide this affirmative defense, but chose not to do so, citing Fed. R. Civ. P. 8(c). Medzam objects to this exercise of judicial restraint, arguing that the validity issue was fully litigated and that it is entitled to a decision, referring in its brief to its "request for a declaration of invalidity or unenforceability."

Although viewed by Medzam as a mere technicality, it is dispositive that Medzam did not file a counterclaim for a declaration of invalidity. The Supreme Court in *Cardinal Chem. Co. v. Morton Int'l, Inc.*, 508 U.S. 83, 26 U.S.P.Q.2D (BNA) 1721, 124 L. Ed. 2d 1, 113 S. Ct. 1967 (1993) drew a dispositive distinction between an affirmative defense and a counterclaim for a declaratory judgment. The Court stated: "An unnecessary ruling on an affirmative defense is not the same as the necessary resolution of a counterclaim for a declaratory judgment."

Cardinal Chemical, 508 [**23] U.S. at 93-94, 26 U.S.P.Q.2D (BNA) at 1726. A request for a ruling of invalidity, for example as in Medzam's motion for judgment as a matter of law filed after close of the plaintiff's case, does not convert the defense into a counterclaim; nor does the filing of a trial brief, nor the filing of proposed findings and conclusions on the issue of validity.

In *Cardinal Chemical* the Court held that the Federal Circuit, when reviewing infringement on appeal, should also review the issue of validity when that issue was raised by counterclaim or declaratory judgment and was decided by the trial court, as a matter of serving the public interest in valid patents. However, the Court suggested that appellate review was unnecessary when the issue of validity was raised only as an affirmative defense. 508 U.S. at 93-94, 26 U.S.P.Q.2D (BNA) at 1726. The Court did not discuss whether there should be an obligation on the trial court to decide the issue of validity, when the dispute has been finally disposed of on other grounds. We decline to require the trial court now to decide patent validity, after the controversy has been resolved.

Thus we decline Medzam's request for further proceedings on the issue of validity, [**24] even as we stress the useful general rule that trial courts should decide all litigated issues, in the interest of finality. See *Sinclair & Carroll Co. v. Interchemical Corp.*, 325 U.S. 327, 330, 65 U.S.P.Q. (BNA) 297, 299, 89 L. Ed. 1644, 65 S. Ct. 1143 (1945) (suggesting that it is usually the better practice for the district court to decide validity); accord *Cardinal Chemical*, 508 U.S. at 100, 26 U.S.P.Q.2D (BNA) at 1729 (citing *Sinclair & Carroll* with approval). We take note that if the Federal Circuit had reversed the judgment of non-infringement, the issue of validity would have required remand and decision, perhaps followed by another appeal, and accompanying cost, delay, and inefficiency. However, as this litigation has evolved, Medzam has no justiciable interest in validity. The case is over.

ATTORNEY FEES

The district court's denial of attorney fees under 35 U.S.C. § 285 is subject to reversal only if (1) the finding that this is not an exceptional case is clearly erroneous and (2) the ensuing refusal of attorney fees is an abuse of discretion.

Findings of exceptional case have been based on a variety of factors; for example, [*1482] willful or intentional infringement, inequitable conduct [**25] before the Patent and Trademark Office, vexatious or unjustified litigation, or other misfeasant behavior. See *Rite-Hite Corp. v. Kelley Co., Inc.*, 819 F.2d 1120, 1126, 2 U.S.P.Q.2D (BNA) 1915, 1919 (Fed. Cir. 1987).

Medzam offers three reasons why this case should be deemed exceptional. First, Medzam states that Multiform engaged in bad faith litigation because Multiform "admitted" that Medzam's product did not have a "degradable" envelope. Multiform responds that it always had the good faith belief that Medzam's product was "degradable" in terms of the '266 patent. We agree that Medzam mischaracterizes Multiform's "admission," and that bad faith can not be founded on this issue.

Medzam also argues that it was an act of bad faith for Multiform to add the "means-for" claims to the '266 patent in an attempt to cover Medzam's product. However, it is neither illegal nor bad faith for an applicant to amend the claims in view of a competitor's product. See *Kingsdown Medical Consultants, Ltd. v. Hollister Inc.*, 863 F.2d 867, 874, 9 U.S.P.Q.2D (BNA) 1384, 1390 (Fed. Cir. 1988), cert. denied, 490 U.S. 1067, 104 L. Ed. 2d 633, 109 S. Ct. 2068 (1989) ("Nor is it in any manner improper to amend or insert [**26] claims intended to cover a competitor's product the applicant's attorney has learned about during the prosecution of a patent application."); *State Industries, Inc. v. A.O. Smith Corp.*, 751 F.2d 1226, 1235, 224 U.S.P.Q. (BNA) 418, 424 (Fed. Cir. 1985).

Medzam also states that Multiform committed inequitable conduct by presenting the patent examiner with misleading dictionary definitions during the prosecution of the '266 patent. Medzam states that Multiform cited the dictionary definition of "degrade," while failing to cite the dictionary definition of "degradable," which Medzam says is inconsistent with "degrade." Medzam states that intent to deceive can be

inferred from this action. Although direct evidence of fraudulent intent is not easy to come by, inference without any probative evidence is insufficient to show culpable intent. As discussed in *Kingsdown*, the charge of inequitable conduct before the patent office had come to be attached to every patent prosecution, diverting the court from genuine issues and simply spawning satellite litigation. See *Kingsdown*, 863 F.2d at 876, 9 U.S.P.Q.2D (BNA) at 1391; *Burlington Indus., Inc. v. Dayco Corp.*, 849 F.2d 1418, 1422, 7 U.S.P.Q.2D (BNA) 1158, 1161 [**27] (Fed. Cir. 1988) (the charge of inequitable conduct in every major patent case "has become an absolute plague"). Medzam has not shown that the dictionary definitions were incorrect or misleading or that the examiner was misled.

The district court correctly held that "Medzam has not shown by clear and convincing evidence that Multiform's conduct before the PTO was inequitable." 1995 WL 737929 at *14. Rejecting Medzam's claim that this was an exceptional case, the court declined to award attorney fees. In *S.C. Johnson & Son v. Carter-Wallace, Inc.*, 781 F.2d 198, 201, 228 U.S.P.Q. (BNA) 367, 369 (Fed. Cir. 1986) we explained that "the trial judge is in the best position to weigh considerations such as the closeness of the case, the tactics of counsel, the conduct of the parties, and any other factors that may contribute to a fair allocation of the burdens of litigation as between winner and loser." The denial of attorney fees is affirmed.

No costs.

AFFIRMED

APPENDIX II. S.

**NOTICE OF APPEAL FROM THE EXAMINER TO
THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Docket Number (Optional)

630-015

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on **10-29-2004**

Signature **[Signature]**

Typed or printed name **James L. Lynch**

In re Application of

Saha:

Application Number

09/614,867

Filed

7-12-2000

For

Method and Computer Program for Offering Products

Art Unit

2154

Examiner

Chad Zhong

Applicant hereby appeals to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 1.17(b))

\$ 340.00

☒ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is:

\$ 170.00

☒ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **23-0420**. I have enclosed a duplicate copy of this sheet.

☒ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒ attorney or agent of record.

Registration number **54,763**

☐ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34. _____

[Signature]
Signature

James L. Lynch
Typed or printed name

(908) 277-3333
Telephone number

October 29, 2004
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.191. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

APPENDIX III: RELATED PROCEEDINGS

5

Appellant is unaware of any prior or pending appeal,
or any judicial or interference proceeding which may
10 directly affect, be related to, be directly affected by, or
have a bearing on the Board's decision in this proceeding.